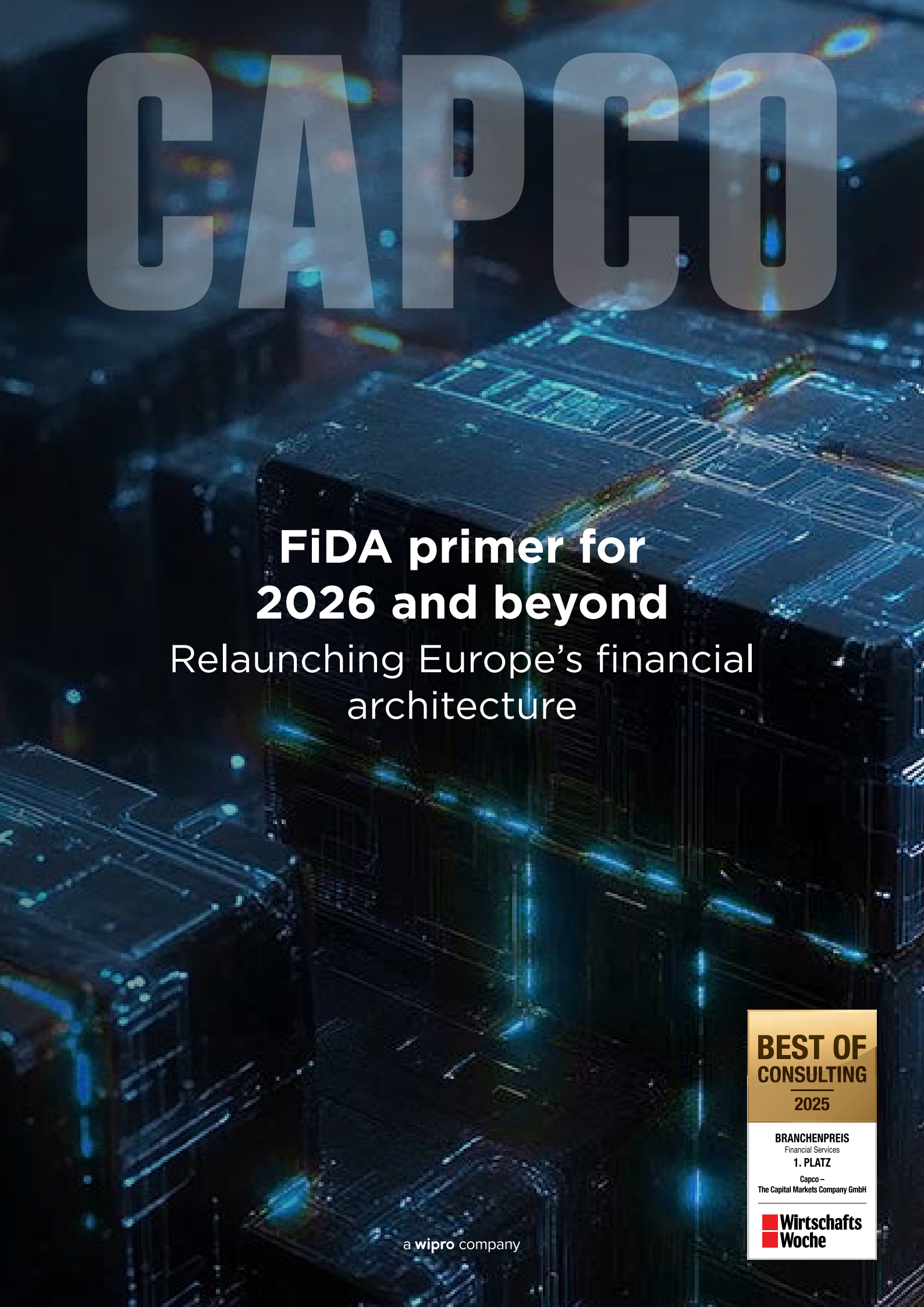


FiDA primer for 2026 and beyond

Relaunching Europe's financial architecture

a **wipro** company

BEST OF CONSULTING
2025
BRANCHENPREIS
Financial Services
1. PLATZ
Capco –
The Capital Markets Company GmbH
Wirtschafts Woche

Table of contents

The Financial Data Access (FiDA) regulation is a key project of the European digital regulation and is already shaping the discussion about Europe's future financial architecture. Aiming to promote innovation and competition, FiDA is designed to create a Europe-wide financial data space for the first time. In the future, banks, insurers, asset managers and other institutions will need to provide (product) data approved by customers in a secure, standardized and controlled manner. In this way, the idea of open banking is transferred to the entire financial industry and at the same time expanded to open finance – all with the overarching goal of creating a trustworthy, interoperable and customer-centric financial data economy. This paper explores FiDA's regulatory context, implementation principles, target operating model and technical foundations, alongside its potential to become a strategic progress driver.

Introduction

FiDA represents a regulatory-led transformation of organizations' IT and data infrastructure, designed to deliver meaningful customer-centric outcomes. Integration instead of siloed solutions, automation and real-time processing instead of manual process flows and customer focus instead of departmental thinking will now be required. Importantly, firms will need to prepare for opening to interoperability on the way to the still distant vision of an open data economy.

Ultimately, FiDA aims to close the gap between technological developments and the evolution of the financial industry, a gap that has grown over the years. In this respect, FiDA is less of a new bureaucratic project and more of a regulatory wake-up call to make up for structural inadequacies.

While regulation increases the pressure to change, it does not replace a clear corporate strategy. FiDA defines framework conditions, while institutions must shape the necessary change themselves. If they approach implementation from a purely compliance-driven perspective, they will face high costs but hardly any benefits.

Only when FiDA is viewed as an opportunity to consistently modernize IT landscapes, anchor clear data responsibility and embed genuine customer centricity can the regulatory imperative translate into strategic progress.

FiDA's focus areas can currently be clustered as follows:

- **Customer interface**
  Previously exclusive customer and product data is becoming available across the market, offering opportunities for customer penetration and acquisition. This also poses risks in the form of potential customer churn, disclosure of internal pricing structures and data (quality) management that is not yet fully mature. Customer centricity is becoming even more important as a key tool for retention and acquisition.

- **From products to platforms**
  FiDA opens data-based business models, e.g. API subscriptions, embedded services or data-driven consulting. The extent of implementation reflects the level of ambition each organization has for FiDA.

  Data owners and data users are potential roles for firms within FiDA. For those who see customer processes, customer data and customer centricity as the new maxim for a digitally driven operating model can use FiDA as the basis to develop their business further towards financial platform providers.

- **From regulation to competition and trust**
  FiDA democratizes financial data as customers gain more transparency and control over their data. For institutions, this means that trust, supported by robust consent processes, auditability and privacy-by-design, is becoming a key competitive factor.

  These three transformation mechanisms mark the shift from the traditional financial sector toward a data-driven financial economy. FiDA provides the regulatory foundation for this new environment - consistent, secure and enabling.

- **Risks and challenges**
  Although the opportunities associated with FiDA are well understood, there are significant hurdles and uncertainties that must not be ignored in the planning process. These include legacy infrastructures, technical complexity, predicting customer behavior and the question of how initial investments can be compensated via monetization and data usage. In addition, there is still uncertainty about the final regulatory framework: the trilogue negotiations (between the European Parliament, the Council of the EU and the European Commission) may entail adjustments to the scope of application, deadlines or role definitions.

A successful FiDA transformation path therefore requires not only a strategic vision, but also robust risk mitigation, the ability to iterate and realistic milestones.

Regulatory context

FiDA is part of the European Commission's Digital Finance Package and complements key regulations such as the Payment Services Directive 3 (PSD3), the Payment Services Regulation (PSR), the Digital Resilience Regulation Act (DORA) and the European Digital Identity (EUDI) wallets framework. Together, these regulations create the legal and technical framework for a modern, secure and innovative financial infrastructure.

FiDA goes beyond payments and establishes a horizontal data access framework for all financial products from accounts to loans, insurance to pensions (and in the future, crypto assets). This makes FiDA the logical continuation of PSD2, but with a much higher demand. While PSD2 opened payments, FiDA opens the entire financial ecosystem. And it does so while laying the foundation for the EU's broader open data economy.[1]

Dovetailing with other regulatory projects

Since FiDA focuses on data-sovereign access, dovetailing with the other parts of the Digital Finance Package is of enormous importance. PSD3/PSR, DORA, EUDI and the General Data Protection Regulation (GDPR) are particularly noteworthy here.

PSD3 and the accompanying PSR modernize the legal framework for payment services. The focus is on consumer protection, fraud prevention and the harmonization of technical requirements, in particular on stable and documented APIs and transparent customer authentication.

DORA defines comprehensive requirements for digital operational resilience, including incident management, ICT risk management, outsourcing management and business continuity requirements. Derived from operational risk management, DORA requires monitoring of information technologies with regard to threats to confidentiality, integrity and availability. This also explicitly includes incident reports, restore/failover samples and third-party control.

In addition to compliant digitalization of payment services and operational risk, the **digital identity with eIDAS,** in particular the EUDI wallet, takes on an important function in customer authentication, which opens the possibility for EU citizens to securely share and sign verifiable proofs.

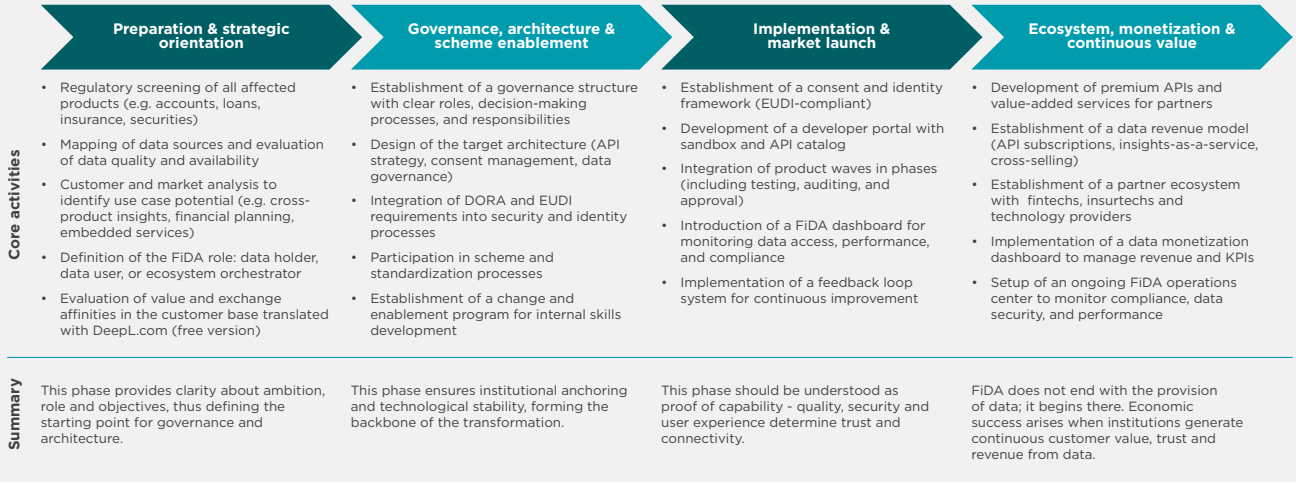
And finally, the **GDPR** unifies data protection in the EU as a further pillar, defining legal bases, purpose limitation, data minimization and data subject rights as well as requiring transparency and accountability.

FiDA thus acts as a connecting layer between identity, security and market mechanisms, making it possible to realize efficiency, trust and market potential at the same time, in an integrated way.

1. Open Finance - What can an enabling framework look like? https://www.europarl.europa.eu/RegData/etudes/STUD/2023/754188/IPOL_STU(2023)754188_EN.pdf

Four phases of FiDA implementation

FiDA requires enterprise-wide transformation across strategy, governance, architecture, data management and monetization. To make this complexity manageable, a four-phase implementation framework is recommended that ensures momentum and synchronization.



Risk horizon across all phases

The four transformation phases offer a structured process, but many risks unfold across phases. They will influence decisions across several dimensions at the same time and, if there is no sufficient control, can destabilize the entire transformation path.

Strategic and regulatory risks arise primarily from the uncertainty in the trilogue negotiations, different national interpretations or an unclear definition of the scope. Such shifts can affect implementations or force expensive adjustments in later phases. Early scenario planning, close monitoring and structural flexibility in processes and architecture are crucial here.

Architecture and technology risks typically arise from rash or flawed design decisions, with incompatibilities, unnecessary complexity or performance problems often being the result. Experience shows that proof-of-concepts, modular architectures and targeted interoperability tests significantly reduce the risk.

Data, consent and data protection risks concern the consistency of the mechanisms that make FiDA functional in the first place. Unclear consent structures, poor data quality or insufficient auditability can cause both regulatory and operational risks. Data security-by-design, clear quality standards and a uniform consent framework are central preventative factors.

Organizational and governance-related risks arise from resistance, lack of role clarity and siloed structures. Without a resilient governance model with defined responsibilities, escalation paths and feedback loops, the transformation loses speed and controllability.

Cost, time and resource risks are present in almost every institution. Budget restrictions, limited specialist resources and ambitious schedules necessitate clear prioritization. Without sufficient control, the risk of suboptimal architecture or implementation decisions increases. Phased financing, clean capacity planning and consistent milestone management form the basis for stability here.

Risks in scaling and market impact primarily affect economic success. Monetization models may prove to be less viable than planned, ecosystems may emerge more slowly than expected or customers may be reluctant to adopt new services.

Recommendations

Clear triggers, escalation mechanisms and mitigation plans should exist for every risk. A central FiDA risk register with responsibilities, degrees of impact and priorities creates the necessary transparency. Regular reviews, especially at phase transitions, will ensure adaptability and prevent early misjudgements from causing high follow-up costs later on.

Alternative route: minimum implementation (compliance-first approach)

Instead of pursuing a comprehensive transformation path, some institutions deliberately choose a minimum-implementation approach, focusing solely on regulatory imperatives: mandatory APIs, consent mechanisms, authorization and basic security requirements.

This approach offers clear advantages: lower complexity, faster implementation and earlier regulatory compliance. Particularly in organizations with significant legacy systems or limited resources, it can initially create stability.

At the same time, however, it is not a substitute for a long-term strategy. A pure compliance approach carries the risk of lock-in later on. Architecture decisions that only meet the minimum today can hinder expansion tomorrow or require expensive refactoring. Differentiation in the market, monetization and data-driven business models also remain limited.

Therefore, the minimum path can be a useful starting point, but only if it is supplemented by a modular architecture and governance roadmap that allows for subsequent expansion stages. Compliance-first must not mean that innovation is permanently excluded.

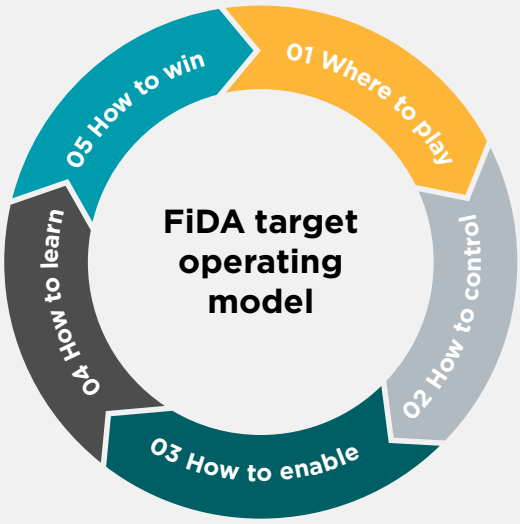
FiDA's long-term benefits

FiDA is not a simple implementation program, but a coordinated, company-wide transformation. The four phases provide a clear framework for translating complexity into manageable steps, from strategic alignment, governance and architecture to operational implementation and monetization. It is crucial to think of the transformation not in purely regulatory terms, but as a business and technology opportunity.

Only those who implement FiDA end-to-end and manage risks appropriately, will benefit in the long term from better customer access, higher data quality, more stable architectures and new revenue models.

The backbone of the FiDA transformation: Target operating model and governance

FiDA not only changes the technical infrastructure but also forces institutions to realign their entire control logic across governance, processes, role models and responsibilities. Traditional financial organizations are often fragmented. An integrated, cross-functional operating model is required to unite governance, technology, data and business in a coherent control system.



	Core elements
01 Strategic level	• Strategic anchoring in the overall corporate strategy • Development of the FiDA vision, including use cases and a consistent roadmap • Definition of governance principles • Prioritisation of business areas, sales channels and partner strategies
02 Governance & compliance level	• Monitoring of regulatory developments (trilogue negotiations, EBA, ESAs) • Risk management, data protection and audit management • Interface with legal and compliance departments • Regular reporting to management
03 Architecture & technology level	• Development of a FiDA architecture blueprint • Establishment of APIs, eventing, data mesh/lakehouse • Integration of EUDI identity systems • Implementation of DORA requirements (operational resilience, security, third-party risk)
04 Data & analytics level	• Development of a company-wide data fabric • Introduction of a data governance framework • Use of AI for data quality and predictive compliance • Integration of customer analytics and propensity models
05 Business & monetization level	• Development of premium API offerings • Design of pricing models and licensing structures • Establishment of a partner portal and developer ecosystem • Integration of data-as-a-service models

Elements of the FiDA target operating model

The FiDA target operating model (TOM) comprises five closely interlinked control levels, which together form the organizational, technological and economic framework for successful FiDA implementation. Each level has clearly defined tasks, responsibilities and KPIs and contributes to making FiDA not only compliant, but strategically effective.

Strategic control level (‘where to play’)

The strategic level determines the role of the institution in the emerging open finance ecosystem. It defines the level of ambition and vision, prioritized use cases and a roadmap that closely links FiDA with the business strategy. At this level, central decisions are made, for example, on the role of the institution in an open finance world, on partnerships and on market-effective positioning. This ensures that the FiDA transformation is not solely compliance-driven but also contributes to clear business strategic goals.

Governance and compliance level (‘how to control’)

This layer ensures that regulation, security and transparency are guaranteed at all times. It monitors regulatory developments (including EBA, ESAs, trilogue negotiations) and translates them into internal guidelines. This is where risk management, data protection, consent processes and auditability are anchored and the interface between specialist departments and compliance is defined. Continuous reporting creates the basis for controllability, trust and regulatory resilience.

Architecture and technology level (‘how to enable’)

The technological level forms the backbone of the FiDA operating model. It includes the development of the FiDA architecture (APIs,

events, data storage and access), the integration of EUDI wallet identities and the implementation of the DORA requirements in terms of resilience, security and third-party risks. The goal is a modern, interoperable infrastructure that breaks down silos, creates real-time capability and enables seamless data delivery.

Data and analytics level ('how to learn')

The data layer focuses on creating value from data. This includes the development of a company-wide data strategy, robust data governance frameworks and the use of analytics and AI, for example for data quality, predictive compliance or customer-centric evaluations. Further, by adding customer analytics and propensity models, organizations can create the foundation for making FiDA profitable.

Business and monetization level ('how to win')

FiDA translates this level into economic success. This includes the development of new data-based business models from premium APIs and embedded services to data-driven consulting and licensing models. It also forms the framework for partner and developer ecosystems as well as for data-as-a-service offerings. The aim is to develop a scalable value-creation model based on the regulatory obligation and to actively shape the firms' market positions in the emerging financial data economy.

Critical reflection on the operating model

A FiDA-compliant operating model is a prerequisite for scalability and controllability, but at the same time its design entails inherent risks. A central area of tension arises from how roles and power are distributed across the levels. If, for example, the technology or compliance function have too much power within a project, then there is a risk that the TOM will be skewed, affecting business requirements, customer expectations or economic potential. Equally critical is the lack of clearly defined responsibilities at the interfaces, which can lead to duplicate structures, gaps in data governance or inefficient escalation paths.

In addition, experience from comparable transformation programs shows that TOMs are often thought of too technically. The result: processual, organizational and cultural success factors are underestimated. Without a well-founded change architecture and established feedback loops, the TOM remains a theoretical construct that does not work in day-to-day operations.

Another risk factor is the lack of iteration capability. A statically designed TOM cannot sufficiently anticipate regulatory adjustments, market changes or new platform ecosystems.

The critical conclusion is therefore that a TOM will only be effective if it is managed in a balanced, adaptive and interdisciplinary manner, and if technical excellence is accompanied by organizational maturity.

IT architecture and data management – FiDA's technical foundation

Architecture is a decisive success factor in the context of FiDA, as it brings together interoperability, trust and regulatory certainty. It overcomes the fragmentation of existing data silos by establishing common standards for data models, interfaces and access mechanisms. This is the only way to enable a controlled, secure and traceable exchange of data between financial institutions, third-party providers and customers.

The integration of the DORA and PSR requirements ensures that only resilient, regulated actors participate in the data traffic. In this way, architecture becomes a strategic lever that combines technology, regulation and trust to form a stable financial data space.

Functional target vision of the FiDA architecture

The FiDA architecture follows a functional vision that combines four central components: data storage, data exchange, consent mechanisms and regulatory monitoring. Together, these elements create the technical and operational foundation for a secure, interoperable and trusted financial data space.

Hybrid data storage

The data layer forms the foundation of the architecture. It links decentralized data sources via semantic models, metadata repositories and data catalogs to form a uniformly addressable database. Data remains anchored in the institutions' domains, while quality, ownership, and retention policy are centrally controlled via governance rules. This creates a federated data architecture that combines openness and control.

Standardized data exchange

The standardized API is the central technical enabler of FiDA. It translates regulatory requirements into interoperable, secure and auditable data interfaces, including versioning, authentication and monitoring. It enables secure, auditable data exchange between financial institutions, financial information service providers (FISPs) and other regulated entities. Data is provided and consumed via clearly defined REST endpoints, including authentication, versioning and monitoring. The API thus operationalizes the regulatory requirements of FiDA and PSR and creates interoperability without centralization.

Consent management

Consent management combines technical governance with user-centric control. FISPs access consent management via REST interfaces, while end customers can manage their approvals transparently via the consent dashboard. Strong Customer Authentication (SCA) secures the process and ensures that access is only based on valid, authorized consent. This creates an end-to-end connection between identity, consent and data use.

Compliance portal

To ensure regulatory traceability, the compliance portal complements the architecture with an institutional view of compliance, auditing and security. This is where accesses, transactions and consent changes are logged, analyzed and reported. The portal enables financial institutions and supervisory authorities to monitor FiDA data flows transparently and in an audit-proof manner, thus forming the backbone of operational governance.

Architectural risks and a 'minimal architecture' option

The introduction of FiDA carries risks due to excessive complexity, insufficient standardization and legacy systems. Further, a lack of modularity and superficial consent implementations can jeopardize compliance and interoperability.

A minimal architecture option can be a starting point, concentrating on three core building blocks:

1. A standardized API layer with a central gateway and monitoring

2. A consent and identity module for governance and transparency

3. A virtual data platform for harmonized data products.

This basis can be gradually expanded to include AI, event and analytics functions without overloading existing systems.

AI integration in the architecture model

In the FiDA context, artificial intelligence is not merely an additional technology component, but rather a consistent architectural principle. Its integration must therefore be controlled, native and implemented across all layers of the FiDA architecture. At the data level, this means establishing clearly defined data structures, including feature stores, embeddings and optional vector memory, which enable semantic searches and contextual queries. These functions can be provided to the application level as synchronous or streaming-based inference services via standardized API and event interfaces.

In the platform and operating environment, the use of AI requires robust MLOps (machine learning operations) framework that includes CI/CD (continuous integration/continuous delivery) for models, model registries, automated testing and observability mechanisms for drift and bias detection. Governance, security and compliance, including identity and consent management, purpose limitation, role models, audit trails and policy-as-code, must be an integral part of these operational processes. In particular, the requirements of GDPR and DORA set clear guidelines for transparency, security and traceability.

In order for AI to be used responsibly and effectively, the system also needs mechanisms for human-in-the-loop, comprehensible explainability and firmly defined feedback loops for technical validation. Non-functional requirements such as robustness, latency and cost control must be explicitly specified. In this way, AI is embedded in the existing service and process landscapes in a modular, reusable and audit-proof manner.

Data management and governance

Resilient data management forms the operational basis for FiDA implementation. Data catalogs, metadata repositories and consent systems act as central reference points (single source of truth) for all relevant data objects. Supplemented by clearly defined data retention policies, a consistent business glossary, a binding ontology and a semantically uniform database are created across all domains.

AI-supported quality mechanisms identify anomalies, inconsistencies and potential violations at an early stage, thus strengthening the integrity and reliability of the data. Governance follows a federated approach. While operational responsibility remains anchored in the individual domains, central guidelines for data quality, access, security and transparency ensure uniform control. This combination of local autonomy and clear regulatory orientation enables innovation without jeopardizing compliance requirements.

Architecture as a basis for sustainable compliance, innovation and competitiveness

The architecture is not only a technical prerequisite, but also the decisive strategic lever for a functioning financial data economy.

Only through a clearly structured interplay of data storage, standardized data exchange, consent control, compliance functionalities and AI integration can a resilient, interoperable and trustworthy FiDA data space be created.

At the same time, the risks – from excessive complexity to inadequate governance – reveal how quickly a FiDA architecture model can become imbalanced. A modular, scalable and deliberately minimal initial architecture therefore forms the most pragmatic starting point, which can be gradually expanded to include analytics, event and AI capabilities.

In this way, architecture becomes more than a technical foundation. It is the regulatory framework that brings together regulation, technology, security and economic value creation. Institutions that anchor FiDA in an architecturally consistent, controlled and future-oriented manner will create the basis for sustainable compliance – and for real innovation and competitiveness in an open financial data economy.

Conclusion: designing FiDA pragmatically – reality, success factors and a minimum path

FiDA is a balancing act between regulation, market and trust. It is not only a regulation, but also a strategic design framework for data-driven, customer-centric business models. Institutions that treat FiDA exclusively as a compliance project are squandering considerable market potential. Only when regulation, technical implementation and market logic are brought together in a coherent bigger picture does real added-value arise.

In reality, however, many institutions find themselves caught between conflicting requirements - complex legacy architectures, tight schedules, unclear regulatory details and high customer expectations for secure data handling. FiDA therefore requires prioritization, strategic clarity, focus on resources and the ability to make iterative adjustments.

Critical success factors – what FiDA really supports in practice

In practice, the following factors form the backbone of a resilient FiDA transformation. They reflect not only the regulatory requirements, but also the experience gained from real transformation projects, highlighting the levers where FiDA programs typically either fail or become successful.

- **Customer-centric process design instead of purely technical implementation.** FiDA is ultimately a customer interface matter. Processes, identities and consent mechanisms must be designed in such a way that they are transparent, trustworthy, intuitive and error-free. Technology follows the process, not the other way around.
- **Empowering employees and reducing uncertainty.** New roles, new data responsibilities and new regulatory mechanics create uncertainty. Without training, communication and clear responsibilities, mistakes, shadow processes or resistance arise.
- **Anchored, cross-functional governance.** FiDA affects compliance, IT, data governance, product and sales. Governance that is located in only one function inevitably leads to imbalances. A policy and procedure framework that integrates multiple functions is necessary.
- **Robust system architecture and controlled operating models.** A FiDA architecture must be modular, resilient and industry-wide. In reality, projects fail less due to technology and more due to poor integration, fragmentation and inadequate monitoring.
- **Binding standards for data quality and transparency.** Data quality is no longer a ‘nice to have’. Without clearly defined quality rules, metadata structures, validation mechanisms and monitoring, misuse or regulatory risk arises. Data quality is crucial for trust.
- **Integrating AI responsibly into decision-making processes.** AI is taking over tasks that used to be performed by humans. This means that governance, supervision and quality assurance are migrating to the systems. Human-in-the-loop, understandable models and clear escalation mechanisms are essential.

These factors are not merely theoretical; they are critical conditions for FiDA to function in day-to-day operations and avoid becoming an additional layer of bureaucratic complexity.

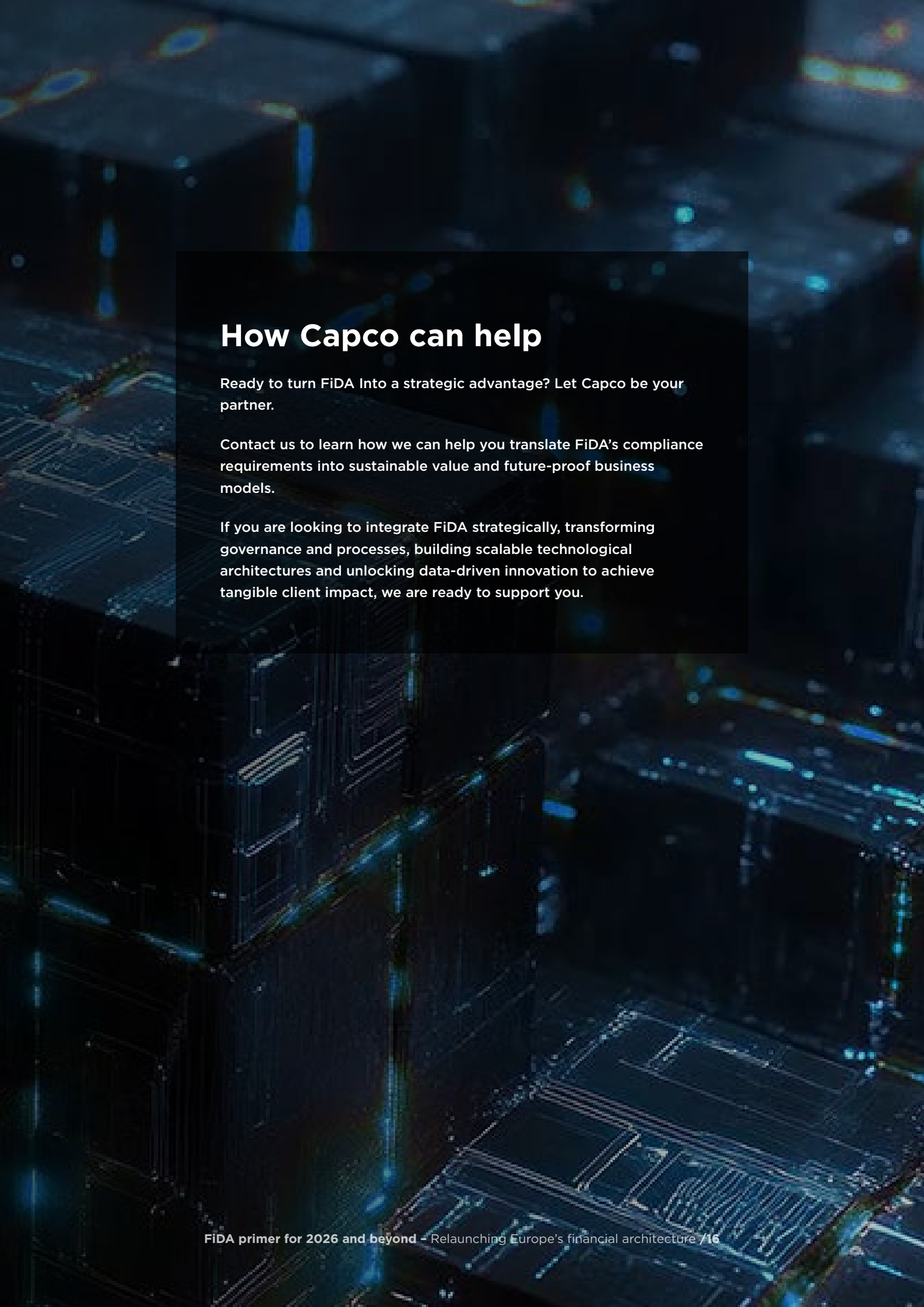
The minimum path as a practical starting point

FiDA is not a straightforward implementation; it must remain a strategically controllable transformation. To achieve that, the minimum implementation path is a logical first step for many institutions. This includes mandatory APIs, consent mechanics and security requirements.

However, a pure compliance approach without an expansion path planned in parallel can lead to a strategic standstill with the risk of being overtaken by market players with more advanced infrastructures.

The most pragmatic approach is to start with a minimum while planning for the maximum from the outset, an approach that is technically modular, organizationally scalable and commercially expandable.

Ultimately, complying with FiDA means not only sharing data, but also aligning architecture, organization and business logic in a future-proof way without losing touch with operational reality.



How Capco can help

Ready to turn FiDA Into a strategic advantage? Let Capco be your partner.

Contact us to learn how we can help you translate FiDA's compliance requirements into sustainable value and future-proof business models.

If you are looking to integrate FiDA strategically, transforming governance and processes, building scalable technological architectures and unlocking data-driven innovation to achieve tangible client impact, we are ready to support you.

Author

Torben Pätz
Managing Principal

Contacts

Jan Stüve
Partner
jan.stueve@capco.com

Torben Pätz
Managing Principal
torben.paetz@capco.com

About Capco

Capco, a Wipro company, is a global management and technology consultancy redefining transformation across the financial services and energy industries. Capco leverages the power of AI and our deep domain expertise to help our clients move faster, make smarter decisions, and drive greater impact. Our award-winning Be Yourself at Work culture and diverse talent drive bold, forward-thinking ideas and lasting change. To learn more, visit www.capco.com or follow us on LinkedIn, Instagram, Facebook, and YouTube.

To learn more, visit **www.capco.com** or follow us on LinkedIn, Instagram, Facebook, and YouTube.

Worldwide Offices

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST
Dubai

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SOUTH AMERICA
Rio de Janeiro
São Paulo

capco.com

CAPCO
a **wipro** company

JN_7402