Roland Berger

Implementation Models for Banks in the Context of the Digital Euro

Author: Zohaib Shaikh

Email: zohaib10092001@gmail.co

Instructor:

Christian Hartmann

January 15, 2026

Abstract:

This research thesis examines the technical architecture, implementation pathways, and strategic models required for banks to integrate the Digital Euro Service Platform (DESP) into their existing infrastructure. The study synthesizes findings from the European Central Bank's preparation phase (2023-2025), industry cost analyses, and technical specifications to provide a comprehensive framework for understanding how different bank tiers—High-tier (large, international), Mid-tier (regional), and Low-tier (small, community)—can adopt the Digital Euro through In-house, Hybrid, or Outsourced implementation models.

The research demonstrates that successful Digital Euro integration depends on technical alignment with the Rulebook Development Group standards, careful cost-benefit analysis of implementation models, and strategic leverage of shared infrastructure and mutualization opportunities. Key findings indicate that costs can be substantially reduced through effective synergy mechanisms. The thesis provides technical blueprints, implementation frameworks, and policy recommendations to guide banks through this critical transition.

1 Introduction

1.1 Background and Motivation

The Eurosystem's Digital Euro initiative represents a fundamental evolution in European monetary infrastructure. As payment behavior shifts toward digital channels and cash usage declines, the European Central Bank (ECB) has initiated a comprehensive project to provide a retail central bank digital currency (CBDC) that complements physical cash while ensuring Europe's monetary sovereignty in an increasingly digitalized economy. The investigation phase (2021-2023) established the conceptual framework for the Digital Euro, exploring design options and distribution models. The subsequent preparation phase (2023-2025) focused on transforming these concepts into operational reality: developing the Digital Euro Scheme Rulebook, selecting technology providers, conducting experimentation through innovation platforms, and validating technical feasibility across diverse use cases including conditional payments and offline functionality.

Europe's payment landscape remains fragmented and vulnerable to external dependencies. Approximately two-thirds of euro area card-based transactions are processed by non-European entities, while 13 euro area countries depend entirely on international card schemes or mobile solutions for in-store payments. The Digital Euro addresses this strategic vulnerability by establishing a pan-European, public digital payment infrastructure that: preserves consumer freedom of choice in payment methods, strengthens European financial autonomy and competitiveness, enables seamless cross-border payments throughout the euro area, provides a foundation for innovation in payment services, and maintains financial inclusion across diverse user segments.

1.2 Research Problem and Objectives

Despite the ECB's comprehensive preparation work, significant uncertainties persist regarding practical implementation for banks:

Primary Research Challenge: How can banks effectively integrate the Digital Euro into their technical infrastructure while managing implementation costs, compliance requirements, and business model adaptations?

Research Objectives:

1. Technical Analysis: Examine the technical architecture of the DESP and required back-end integration patterns for different bank categories
2. Implementation Modeling: Evaluate three distinct implementation approaches (In-house, Vendor/Outsourced, Hybrid) with respect to cost efficiency, scalability, and compliance
3. Bank Tier Stratification: Develop tier-specific implementation strategies addressing the distinct capabilities and constraints of High-tier, Mid-tier, and Low-tier institutions
4. Shared Infrastructure Assessment: Analyze opportunities for cost mutualization through shared services, collaborative platforms, and vendor consolidation
5. Cost-Benefit Analysis: Synthesize findings from multiple cost studies and develop realistic financial projections for different implementation scenarios
6. Policy Implications: Formulate recommendations for banks, regulators, and the ECB to optimize implementation outcomes.

1.3 Research Questions

This thesis addresses the following core research questions:

- RQ1: Technical Integration
    1. How should banks map internal data models and systems to Digital Euro Service Platform requirements?
    2. What are the technical implications of different API protocols and architectural patterns (microservices vs. monolithic)?
    3. How do conditional payments and offline synchronization affect back-end design decisions?
- RQ2: Implementation Models
    1. What are the comparative advantages and disadvantages of In-house, Hybrid, and Outsourced implementation approaches?
    2. How do implementation costs, timelines, and risk profiles differ across these models?
    3. Which implementation model is optimal for each bank tier?

- RQ3: Shared Infrastructure and Mutualization
    1. What cost synergies can be achieved through shared infrastructure and collaborative vendor engagement?
    2. How do market-specific factors (vendor concentration, outsourcing prevalence, collaboration history) influence synergy potential?
    3. What organizational and contractual arrangements facilitate effective cost mutualization?
- RQ4: Risk and Feasibility
    1. What are the primary technical, operational, and financial risks in Digital Euro integration?
    2. How can banks effectively manage the complex interplay between mandatory compliance and optional innovation?
    3. What governance structures and expertise requirements are necessary for successful implementation?

1.4 Research Scope and Methodology

The research focuses on the European Central Bank's (ECB) digital euro initiative, with particular attention to the preparation phase from 2023 to 2025 and the anticipated implementation period between 2025 and 2029. Within this temporal frame, the analysis covers banking systems across the 20 euro area countries, concentrating on retail banks with significant customer bases and differentiating them by asset size and market position. The technical perspective is limited to back-end integration, core system modifications, application programming interface (API) implementation, and compliance-related infrastructure, while front-end user interfaces and broader macroeconomic impact assessments are deliberately excluded from the scope.

Methodologically, the study adopts a mixed-methods design that integrates several complementary approaches to ensure both analytical depth and practical relevance. First, it undertakes a structured document analysis of ECB rulebooks, technical specifications, progress reports, and relevant regulatory frameworks. Second, it synthesizes existing cost studies by incorporating findings from the PwC Digital Euro Cost Study, ECB cost assessment exercises, and estimates from banking associations. Third, it includes technical modeling of functional architectures, API specifications, and data flow diagrams to capture the operational implications of different integration choices. Fourth, the research applies comparative case analysis to examine implementation approaches across diverse banking models and geographic contexts within the euro area. Fifth, it conducts a synergy assessment through quantitative evaluation of mutualization and outsourcing opportunities, relying on structured vendor and partnership analyses. Finally, it develops scenario-based cost and complexity projections across three distinct implementation model scenarios to explore potential outcome ranges under varying strategic and technical assumptions.

2 Background on the Digital Euro: Conceptual and Infrastructural Foundations

2.1 Conceptual Framework and Definitions

2.1.1 Digital Euro: Definition and Functional Characteristics

The Digital Euro, or CBDC, is a digital form of central bank money—specifically, a direct liability of the Eurosystem—available to the general public for electronic payments. It differs fundamentally from commercial bank money, e-money, and private cryptocurrencies:

Table 1: Comparison of Digital Currencies and Money Types

Characteristic	Digital Euro	Commercial Bank Money	E-Money	Cryptocurrency
Issuer	ECB/Eurosystem	Commercial banks	E-money institutions	Decentralized/Private
Legal Status	Central bank liability	Bank liability	Prepaid value	Varies (often unregulated)
Settlement	Real-time, final	Interbank clearing	Custodian-based	Blockchain-based
Privacy	High (pseudonymous)	Low	Medium	Variable
Universal Access	Yes (legal tender)	Conditional (account holders)	Conditional	Open
Regulatory Oversight	Full (ECB)	Full (Banking Supervision)	Moderate	Limited

The digital euro is designed to fulfil several complementary roles within the European payment ecosystem. As a store of value, users can hold digital euro balances, subject to calibrated holding limits intended to safeguard financial stability. As a medium of exchange, it supports seamless transactions in peer-to-peer contexts, at the point of sale, and in e-commerce environments, thereby integrating into everyday payment use cases. Denominated in euros and maintaining one-to-one parity with physical cash, it also functions as a unit of account, ensuring consistency with existing monetary denominations. In addition, the provision of offline payment capabilities is intended to enhance payment system resilience by enabling transactions during temporary network outages. Finally, the digital euro is conceived as a tool for promoting financial inclusion, as it would be accessible to all residents of the euro area, including those without traditional banking relationships.

2.1.2 Key Digital Euro Ecosystem Actors

The Digital Euro ecosystem comprises several interconnected participant categories:

- Eurosystem (ECB)
  - Develops and maintains the Digital Euro Service Platform (DESP)
  - Establishes regulatory standards through the Rulebook Development Group
  - Manages settlement and core clearing functions
  - Ensures system resilience and cybersecurity
  - Does not see end-user identities (privacy-preserving architecture)
- Payment Service Providers (PSPs) - Banks and Non-Bank Operators
  - Distribute Digital Euro services to end users
  - Manage customer onboarding and Know-Your-Customer (KYC) compliance
  - Perform pre-authorization and fraud prevention
  - Handle funding and defunding operations (liquidity management)
  - Provide customer support and dispute resolution
- End Users (Natural and Legal Persons)
  - Individual consumers using Digital Euro for daily transactions
  - Merchants and businesses accepting Digital Euro payments
  - Government entities for tax collection and benefit distribution
  - Operators requiring conditional payment capabilities
- External Service Providers
  - Technology vendors (alias lookup, fraud detection, app development)
  - Platform developers (mobile wallets, payment apps)
  - Security and encryption service providers

- Payment terminal manufacturers

3 Literature Review: Integration of Global CBDC Experience and Technical Standards

3.1 Global CBDC Implementation Experiences

While the Digital Euro represents a unique initiative focused on retail CBDC with sophisticated integration requirements, examining comparable CBDC projects provides valuable insights into technical and organizational challenges.

3.1.1 Comparative Analysis of Retail CBDC Projects

- e-CNY (China Digital Currency Electronic Payment):

  The e-CNY (Digital Currency Electronic Payment) represents the world's largest retail central bank digital currency (CBDC) deployment, initiated conceptually in 2014, with large-scale pilot operations starting in 2020 in selected Chinese cities and regions. Technically, it operates under a two-tier architecture in which the central bank is responsible for issuance and overall infrastructure, while commercial banks and payment service providers manage distribution, customer interfaces, and much of the operational layer. The system supports offline payments via hardware wallets and secure elements embedded in devices, and it incorporates programmable features allowing smart contract–based logic to be linked to transactions, alongside near real-time settlement capabilities in the underlying infrastructure.

  For the digital euro, several key lessons can be drawn from the e-CNY experience. The two-tier model substantiates the strategy of relying on existing payment service providers for distribution, as it leverages established banking and fintech infrastructures while preserving the central bank's control over issuance and settlement. However, the development and deployment of robust offline functionality have proven technically complex, requiring extended design, testing, and certification cycles, especially when hardware-based secure elements and diverse device environments are involved. Coordination with handset manufacturers and other device vendors has emerged as a critical challenge, given stringent security requirements and heterogeneous hardware ecosystems. Moreover, user adoption has depended heavily on strong merchant-side incentives and integration with existing retail payment infrastructures, demonstrating that technical readiness alone is insufficient without clear value propositions for merchants and consumers.

In terms of scale, e-CNY pilots have reached hundreds of millions of transactions by 2024 and have been rolled out across more than twenty pilot cities and regions, with deep integration into retail merchant acceptance networks, including large platforms, small merchants, and public service payments. This breadth of deployment underscores the importance of phased, geographically diversified pilots and close collaboration with large retailers, platforms, and local authorities when planning and implementing a retail CBDC such as the digital euro.

- Bahamas Sand Dollar:

  The Sand Dollar, launched by the Central Bank of The Bahamas in 2020 as the first live retail central bank digital currency (CBDC), was designed for a population of roughly 400,000 and explicitly targeted gaps in financial access and payment resilience in an island economy. Its architecture emphasizes digital wallet provisioning for unbanked and underbanked residents, using a mobile-first design that allows users to access and transact with Sand Dollar balances primarily via smartphones and basic mobile devices, while integrating with existing domestic payment infrastructure and financial intermediaries.

  For a prospective digital euro, several design lessons emerge from the Sand Dollar experience. Embedding financial inclusion objectives from the outset, rather than treating them as secondary benefits, proves crucial in guiding wallet design, onboarding processes, and distribution partnerships. A mobile-first orientation can significantly reduce dependence on costly physical infrastructure and branch networks, especially in regions with uneven access to banking services, although it simultaneously raises the bar for robust cybersecurity, user authentication, and device-level fraud prevention mechanisms. The relatively small scale of the Bahamian deployment has enabled a more controlled, phased introduction of features and risk controls, highlighting the value of constrained pilots and iterative roll-outs even in larger currency areas. Finally, strong user authentication frameworks, combined with effective fraud detection and consumer protection measures, have been essential to building and sustaining public trust in the Sand Dollar as a secure and reliable means of payment.

- Sweden e-Krona Pilot:

  Sweden's e-krona pilot, conducted over an extended period from 2020 to 2024, has concentrated on exploring offline payment capabilities and understanding drivers of retail adoption in a highly digitalized payments environment. The technical design emphasizes mechanisms for executing transactions without continuous network connectivity, while ensuring interoperability with existing electronic payment systems and addressing specific edge cases, such as limited connectivity in rural areas and the needs of elderly or less digitally literate users.

  Several lessons from the e-krona pilot are particularly relevant for the digital euro. First, testing offline functionality demands comprehensive scenario coverage, including diverse device types, network conditions, and user segments, in order to validate robustness and security under real-world constraints. Second, systematic user testing with vulnerable or less digitally experienced populations is essential for identifying accessibility, usability, and support requirements that may not emerge in mainstream user groups. Third, experience in Sweden indicates that integrating merchants and their point-of-sale systems can be more complex than achieving consumer wallet adoption, reflecting the need for tailored merchant onboarding, incentives, and technical support. Finally, the multi-year duration of the pilot—spanning more than three years—has proven valuable in enabling iterative refinement of technology, legal frameworks, and operational processes, suggesting that long pilot phases can substantially improve the maturity and acceptability of a retail CBDC design.

3.2 Technical Standards and Best Practices

3.2.1 Payment Industry Standards Applicable to Digital Euro

The digital euro design builds on established payments industry standards to minimise integration complexity and maximise interoperability across the euro area ecosystem. At the messaging layer, it adopts ISO 20022 as the universal standard for the exchange of payment transaction information, using structured and machine-readable formats that align with existing SEPA payment schemes and infrastructures. The corresponding rulebooks mandate ISO 20022-compliant transaction messaging, ensuring consistent implementation across participants and facilitating reuse of current back-end processing capabilities.

The architecture is further aligned with the experience gained under the second Payment Services Directive (PSD2), particularly in the use of REST-based application programming interfaces (APIs) and related security profiles. By building on familiar integration patterns for payment service providers, this approach reduces learning curves, shortens implementation timelines, and allows institutions to leverage a significant share of their existing technical infrastructure and interface frameworks.

Within the broader scheme landscape, the digital euro is designed to complement, rather than displace, SEPA arrangements, including instant credit transfer services such as SCT Inst, while relying on similar participant structures and governance mechanisms. This orientation supports seamless account-to-account integration and enables coordinated evolution with existing payment schemes instead of creating an entirely separate ecosystem.

For front-end and acceptance-side processing, the design references open standards that already support card, QR-based, and account-based payments. These include CPACE for contactless card payments, relevant standards of the European Payments Council such as those for QR code payments (e.g. EPC024-22) and SEPA Request-to-Pay, as well as nexo standards for terminal and ATM transactions and Berlin Group specifications for mobile peer-to-peer and open finance APIs. Collectively, these standards provide a modular toolkit for integrating the digital euro into existing consumer and merchant channels with limited incremental complexity.

3.2.2 Cybersecurity and Privacy Standards

Cybersecurity and privacy standards for a digital euro must align with European data protection law while ensuring strong technical safeguards against misuse and attacks. In terms of GDPR compliance, the architecture should incorporate pseudonymization of transaction data so that personal identifiers are separated from operational data wherever possible, thereby reducing the risk of direct identification in case of data breaches. Data minimization principles require that only strictly necessary personal information is collected and processed for payment execution, dispute handling, and regulatory obligations, while users retain clear and enforceable control over how their personal data is used, accessed, and retained. These legal and organisational safeguards are embedded through a privacy-by-design and privacy-by-default approach, meaning that default system settings and technical choices are configured to maximise privacy protection throughout the lifecycle of the system.

To further strengthen confidentiality and unlinkability, the design can employ privacy-enhancing technologies that complement baseline GDPR controls. Zero-knowledge proof mechanisms may be used, particularly in offline transaction contexts, to allow validation of transaction legitimacy or balance sufficiency without exposing full transactional or identity details. Blind signature schemes and related cryptographic obscuration techniques can help prevent intermediaries from linking specific users to individual payment events beyond what is strictly necessary. Segregated data processing pipelines, where identity data and transactional data are handled by logically or physically separated components, further limit the scope for unwarranted profiling or cross-linking. In addition, cryptographically secure token-based transfers can ensure that transaction instruments themselves do not leak sensitive information and can be invalidated or refreshed if compromise is suspected.

On the cybersecurity front, the digital euro ecosystem would rely on robust, certifiable security components and state-of-the-art communication protections. Secure elements used in cards, phones, or hardware wallets should meet recognised evaluation benchmarks, such as Common Criteria (CC) at Evaluation Assurance Level 4 (EAL4) or higher, providing assurance regarding resistance to tampering and sophisticated attacks. Communication channels between wallets, intermediaries, and central infrastructure must be protected using modern transport-layer cryptography, for example through TLS 1.3 or later, to safeguard data in transit against interception and modification. Cryptographic key material for the core infrastructure should be generated, stored, and used within hardware security modules, which provide strong isolation and audit capabilities for key management operations. Finally, the overall system security posture must be maintained through continuous monitoring and periodic independent security testing, including penetration tests and red-team exercises, ensuring that newly discovered vulnerabilities are identified and remediated in a timely and transparent manner.

3.3 Cost and Feasibility Studies: Synthesis and Analysis

3.3.1 Primary Cost Research

PwC Digital Euro Cost Study (2025)

Scope: 19 participating banks across euro area (€20-1000+ bn asset range)

Key Findings:

1. Average implementation cost per bank: €110 million
2. Total euro area extrapolation: €18 billion (baseline)
3. High scenario with offline/multiple accounts: €30 billion
4. Technical layer dominates costs: 75 percent of total (€1.5 billion)

Cost Distribution by Service Bundle:

Table 2: Average Costs and Percentages by Component

Component	Average Cost	Percentage
Mobile/Web Frontend	€10 million	8%
ATM Infrastructure	€9 million	7%
Interfaces/APIs	€6 million	5%
POS Terminal Adaptation	€7 million	6%
Account/Liquidity Management	€8 million	6%
Branch Network Adaptation	€3 million	2%
Risk/Compliance Functions	€7 million	6%
Marketing/Customer Contracts	€12 million	10%
Operational Processes	€31 million	25%

Key Caveats:

1. Excludes multiple account functionality
2. Based on rulebook v0.8a (evolution to v0.9 may modify costs)
3. 46 percent of available skilled resources tied up per year for 4 years

ECB Assessment of Digital Euro Investment Costs (October 2025)

Adjusted Baseline Costs (incorporating design adjustments):

- Physical card infrastructure: -€6 million (cards use existing infrastructure)
- POS terminal replacement: -€7 million (natural refresh cycles, smart/soft POS adoption)
- ATM infrastructure: -€5.1 million (existing NFC/QR support, outsourcing to independent ATM deployers)
- Fee calculation component: -€2 million (handled by Eurosystem)
- Overall adjustment: -€20 million per bank (-16 percent)

Adjusted Average Costs by Bank Size:

- Large banks (>€1 trillion assets): €152 million
- Large banks (€100-1000 billion): €89 million
- Medium banks (€30-100 billion): €24 million
- Small banks (<€30 billion): €8 million

Euro Area Total with Synergies:

- Base scenario (30 percent market synergies, 90-98 percent IPS banking group synergies): €4.0-5.77 billion
- High scenario (40 percent market synergies): €5.07 billion
- High scenario (40 percent market synergies): €5.07 billion
- Within European Commission's estimated range (€2.8-5.4 billion)

3.4 Bank Integration Case Studies: Implementation Approaches

3.4.1 In-House Implementation Approach: High-Tier Banks

Typical Profile:

- Large international banks (>€500 billion assets)
- Advanced IT infrastructure and technical capabilities
- Decentralized operations across multiple jurisdictions
- Significant retail customer base requiring sophisticated features

Integration Characteristics:

- Full proprietary development of interfaces and middleware
- Custom microservices architecture enabling feature agility
- Integrated fraud detection and risk management systems
- Advanced analytics for real-time transaction monitoring
- Dedicated Digital Euro business units with specialized teams

Cost Implications:

- Higher upfront development costs (€150-200 million range)
- Internal resource allocation: 50-60

- Lower long-term operating costs through proprietary optimization
- Ability to extract competitive advantages through feature differentiation

Risk Profile:

- Significant execution risk: large, complex technical programs prone to delays
- Resource scarcity: diverts talent from other innovation initiatives
- Maintenance burden: responsibility for entire integration stack
- Regulatory compliance: direct accountability for all security requirements

3.4.2 Vendor/Outsourced Approach: Low-Tier and Mid-Tier Banks

Typical Profile:

- Smaller regional or community banks (€10-100 billion assets)
- Limited IT development capacity
- Reliance on third-party service providers for core systems
- Focus on traditional banking relationships and local markets

Integration Characteristics:

- Engagement with established vendors providing Digital Euro platforms
- Minimal in-house development; integration focused
- Reliance on vendor-provided compliance and fraud detection
- Limited customization; acceptance of standard feature sets
- Licensing or SaaS-based engagement models

Vendor Ecosystem:

- Pan-European providers: Worldline, Nexi, Temenos
- National champions: SIBS (Portugal), Redsys (Spain), CBI (Italy)
- Specialized players: equensWorldline, Sapient, Almaviva
- Cooperative bank platforms: Atruvia (Germany), Argenta (Austria)

Cost Implications:

- Lower upfront development costs (€20-50 million range)

- Vendor licensing/SaaS fees (ongoing operational costs)
- Reduced internal resource burden (10-20
- Shared infrastructure costs distributed across multiple users
- Reduced synergy potential: limited vendor selection creates lock-in

Risk Profile:

- Vendor dependency: migration costs if vendor relationship changes
- Feature limitations: constrained to vendor-provided capabilities
- Vendor stability: operational disruption risk if vendor fails
- Reduced competitive differentiation: identical feature sets across multiple banks

3.4.3 Hybrid Approach: Mid-Tier Banks with Strategic Positioning

Typical Profile:

- Mid-sized banks seeking balanced efficiency and differentiation (€50-300 billion assets)
- Partial internal IT capabilities with selective outsourcing
- Strategic focus on specific value-added services
- Interest in differentiated customer offerings while managing costs

Integration Characteristics:

- Outsourced core integration through established vendors
- In-house development of proprietary value-added services
- Custom integration of existing core banking systems
- Selective build vs. buy decisions based on competitive advantage potential
- Collaborative engagement with peer institutions for shared infrastructure

Value-Added Service Examples:

- Enhanced conditional payment capabilities for B2B use cases
- Loyalty program integration and merchant incentive structures
- Supply chain payment solutions and working capital optimization

- Cash management and liquidity forecasting
- Advanced fraud prevention and financial crime detection

Cost Implications:

- Moderate upfront costs (€60-120 million range)
- Blended vendor licensing and internal development
- Significant resource allocation (30-40
- Phased implementation: core integration via vendor, enhancements over time
- Medium-term savings through selective internalization of high-value functions

Risk Profile:

- Balanced approach: reduced vendor dependency while managing development complexity
- Technology integration challenges: connecting vendor platform with proprietary systems
- Governance complexity: managing internal development alongside vendor relationship
- Organizational alignment: requires clear business/technical strategy coordination

4 Technical Architecture of DESP and Bank Back-End Integration

4.1 DESP Architecture Overview and Core Components

4.1.1 Structural Design Principles

The DESP embodies several fundamental architectural principles that shape integration requirements for banks:

- **Distributed, Segregated Architecture**
  - No single point of failure: components distributed across multiple providers and regions
  - Data segregation: user identities separate from transaction data

  - Processing segregation: distributed across multiple DESP components
  - Enables both resilience and privacy protection
- **Stateful Transaction Processing**
  - Server maintains transaction state throughout processing lifecycle
  - Reduces complexity vs. stateless approaches
  - Enables faster processing and automatic recovery from failures
  - Simplifies bank back-end integration requirements
- **Two-Tier Settlement**
  - Settlement layer (Eurosystem): maintains authoritative ledger, executes final transfers
  - Conditionality layer (market participants): implements conditional payment logic
  - Enables flexibility for innovation while ensuring settlement certainty
- **REST API Standardization**
  - Synchronous REST interfaces between PSPs and DESP
  - Familiar to PSPs from PSD2 implementation experience
  - Enables real-time processing at scale
  - Reduces implementation complexity vs. proprietary protocols

4.1.2 Core DESP Services and Functions

Access Management Service

- User onboarding and provisioning workflows
- Wallet creation and activation
- Alias management and resolution
- Authentication credential setup
- Device provisioning for offline capability
- Waterfall account configuration

Integration Requirement: Bank systems must capture user identity information, perform KYC/AML verification, and transmit verification status to DESP via standardized APIs.

Liquidity Management Service

- DCA account management and monitoring
- Waterfall funding mechanism: PSP DCA → user wallets
- Reverse waterfall: linked commercial bank account funding
- Automatic liquidity replenishment triggers
- Settlement lag management and collateral requirements

Integration Requirement: Bank treasury systems must interface with DESP liquidity management, supporting real-time liquidity monitoring, automated funding triggers, and cash position management.

Transaction Management Service

- Payment instruction processing
- Multi-channel support: POS, e-commerce, P2P, offline
- Pre-authorization and fraud verification
- Transaction state management
- Clearing and settlement coordination
- Transaction history and reporting

Integration Requirement: Bank authorization, switching, and clearing systems must integrate with DESP transaction management, supporting real-time authorization, clearing coordination, and comprehensive audit trails.

Offline Service

- Secure element provisioning and management
- Offline wallet creation and fund loading
- Device-to-device transaction processing

- Offline transaction recording and token management
- Automatic reconciliation upon reconnection
- Recovery mechanisms for device loss or duplication

Integration Requirement: Bank mobile banking and device management systems must support secure element provisioning, offline wallet management, and integration with device manufacturers' secure element APIs.

Risk and Compliance Service

- Fraud detection and prevention
- Risk scoring and transaction monitoring
- AML/CFT compliance verification
- Dispute detection and flagging
- Pattern analysis and behavioral monitoring
- Regulatory reporting support

Integration Requirement: Bank compliance, fraud detection, and risk management systems must ingest DESP risk signals, provide real-time transaction scoring, and execute dispute management procedures.

4.2 Bank Back-End System Integration Pathways

4.2.1 Core System Integration Architecture

Banks must integrate the DESP with existing back-end systems across multiple dimensions:

Core Banking System Integration

- Account master data synchronization
- Customer KYC/AML profile integration
- General ledger and accounting records
- Customer statement and reporting

- Balance management and limit enforcement
- Interest and fee calculation

Middleware and Integration Layer

- API gateway for DESP connectivity
- Message queue systems for asynchronous processing
- Data transformation and mapping services
- Orchestration engines for multi-step workflows
- Event processing and notification systems
- Caching layers for performance optimization

Front-End Distribution Channels

- Mobile banking application integration
- Web portal modifications
- ATM network integration
- Branch banking system connections
- POS terminal ecosystem
- Merchant and customer communication channels

Back-Office and Operational Systems

- Treasury and liquidity management
- Compliance and AML screening
- Fraud detection and prevention systems
- Dispute management and resolution
- Customer service and support systems
- Financial reporting and regulatory submission

4.2.2 Data Model Mapping and Transformation

The DESP operates with specific data models that banks must map to internal representations:

Digital Euro Account Number (DEAN)

- Unique identifier for each Digital Euro account
- Assigned by DESP upon account creation
- Distinguished from user identity (which remains with PSP)
- Used for transaction routing and settlement

Bank Integration Requirement:

- Customer ID (Bank Internal) → [Mapping] → DEAN (DESP)
- Maintained in bank customer reference file
- Used for all Digital Euro transactions
- Updated during wallet provisioning/deprovisioning

Alias-to-DEAN Mapping

- Users can register aliases: phone number, email, IBAN
- Alias Lookup Service (DESP component) maintains alias registry
- Banks responsible for alias validation and user consent management
- Requires integration with identity verification systems

Bank Integration Requirement:

1. Alias Registration Request
2. Validate user ownership of alias
3. Submit to DESP Alias Lookup Service
4. Maintain local mapping for rapid resolution
5. Support alias-based payment initiation

Transaction Message Formats

- ISO 20022-compliant transaction messages
- Structured, machine-readable formats
- Includes transaction type, amount, payer/payee identification, conditionality flags
- Supports various use cases: P2P, POS, e-commerce, conditional

Bank Integration Requirement:

1. Transaction Initiation (Bank Format)
2. Transform to ISO 20022 format
3. Submit to DESP via REST API
4. Parse response and update local systems
5. Provide confirmation to payer/payee

Pseudonymization and Privacy Safeguards

- Banks transmit transactions using DEAN (not customer name or identity)
- DESP cannot link transactions to individuals
- Enables regulatory oversight without privacy intrusion
- Requires careful data separation in bank systems

Bank Integration Requirement:

- Customer Identity (Bank Secret) $\neq$ DEAN (DESP Visible)
- Transaction Processing Uses DEAN Only
- Maintains user privacy to ECB/Eurosystem
- Enables compliance reporting without identity linkage

4.2.3 Liquidity Management Integration: DCA Operations

DCA Account Structure

- Individual DCA held by each PSP at respective NCB
- Functions as liquidity reserve for Digital Euro distribution

- Reconciled daily during DESP settlement processes
- Subject to reserve requirement calculations (similar to other central bank deposits)

Waterfall Funding Mechanism **Typical Waterfall Sequence:**

1. Customer initiates Digital Euro purchase (DESP wallet funding)
2. Bank validates customer has sufficient commercial bank funds
3. Bank debits customer commercial bank account
4. Bank credits own DCA at NCB
5. DESP transfers Digital Euro from central reserve to customer DEAN account
6. Bank records transaction in both commercial and Digital Euro accounting

Integration Requirements:

- Real-time visibility of DCA balance
- Automated funding triggers based on Digital Euro demand
- Integration with automated clearing house (ACH) systems
- Reserve calculation including Digital Euro distribution
- Daily reconciliation with NCB settlement records

Reverse Waterfall (Customer-Initiated Withdrawal) **Reverse Waterfall Sequence:**

1. Customer initiates Digital Euro conversion to commercial bank account
2. DESP debits customer DEAN account
3. Bank receives Digital Euro credit to DCA
4. Bank credits customer commercial bank account
5. Bank reconciles DCA with NCB records
6. Cash settlement through standard central bank procedures

Integration Requirements:

- Bi-directional funding capability
- Automated clearing of reverse waterfall requests
- Integration with settlement systems

- Compliance with holding limit enforcement (prevents excessive conversion)
- Operational risk management (fraud, duplicate requests)

4.2.4 Multi-Channel Integration: Enabling Diverse Payment Methods

Banks must integrate Digital Euro capabilities across multiple customer interaction channels:

POS (Point-of-Sale) Integration

- Terminal support for NFC, QR code, and link-based payments
- Real-time authorization with fraud detection
- Immediate transaction settlement confirmation
- Merchant confirmation and receipt generation
- Integration with existing merchant acquiring infrastructure

Integration Complexity: HIGH

- Requires terminal vendor coordination
- Hardware upgrades for older terminal types
- Software updates and certification
- Network redundancy for resilience
- Merchant training and support

E-Commerce Integration

- Payment page modifications for Digital Euro option
- DEAN or alias-based payment authorization
- M-commerce support (mobile app with redirect flows)
- Pay-by-link capabilities (merchant generates payment link)
- Session management and transaction linking
- Tokenization for recurring payments

Integration Complexity: MEDIUM

- API-based integration (familiar to banks)
- Minimal infrastructure changes
- Standard payment gateway modifications

P2P (Peer-to-Peer) Integration

- Mobile banking app modifications
- DEAN and alias-based payment initiation
- QR code generation and scanning
- Contact-based recipient identification
- Transaction confirmation and receipt

Integration Complexity: LOW

- Mobile app feature additions
- Minimal back-end changes
- Leverages existing P2P infrastructure
- Natural extension of mobile banking

ATM Integration

- Funding and defunding capability
- QR code and NFC support
- Real-time connection to liquidity management
- Security and fraud prevention
- Older ATM compatibility (QR code vs. hardware NFC)

Integration Complexity: MEDIUM–HIGH

- ATM network coordination challenges
- Hardware replacement for NFC support
- Network resilience requirements
- Cash handling reconciliation

5 Implementation Models: Technical and Strategic Analysis

5.1 In-House Implementation Model: Architecture and Requirements

5.1.1 Model Characteristics and Applicability

Ideal Bank Profile:

- Large, internationally active banks (typically >€300 billion assets)
- Advanced IT infrastructure and development capabilities
- Significant technical staff and specialized expertise
- Decentralized operations requiring customization
- Strategic need for competitive differentiation
- Sufficient capital for substantial upfront investment

Key Characteristics:

- Full proprietary development and maintenance responsibility
- Complete control over feature development and timelines
- Direct accountability for security and compliance
- Maximum flexibility for customization and innovation
- Highest development and operational complexity

5.1.2 Technical Architecture for In-House Implementation

Microservices Architecture Approach

Microservices Components:

1. **Access Management Service** — Functions: onboarding, wallet provisioning, alias management. Tech: Java/Spring Boot, PostgreSQL. API: user creation, verification, wallet activation. Dependencies: core banking, KYC/AML.

2. **Liquidity Management Service** — Functions: DCA monitoring, waterfall operations, funding triggers. Tech: Node.js, MongoDB, Redis. API: DCA balance, waterfall request, reverse waterfall. Dependencies: treasury, settlement, DESP.
3. **Transaction Management Service** — Functions: transaction processing, clearing, settlement coordination. Tech: Java, Kafka, PostgreSQL. API: payment instruction, authorization, clearing. Dependencies: auth, clearing houses, fraud detection.
4. **Risk and Compliance Service** — Functions: fraud detection, AML screening, risk scoring. Tech: Python (AI/ML), Apache Spark, feature store. API: risk scoring, flagging, compliance reporting.
5. **Offline Management Service** — Functions: secure element provisioning, offline wallet management. Tech: C++, HSM integration. API: secure element provisioning, offline wallet creation.

Integration with Existing Systems:

5.1.3 Development and Deployment Considerations

Team Structure and Expertise Requirements:

Role	Required FTEs	Key Expertise
Platform Architects	2–3	Cloud architecture, microservices, system design
Backend Developers	15–20	Java, Python, API development, database design
DevOps Engineers	5–8	Kubernetes, CI/CD, infra automation, monitoring
QA/Testing Engineers	8–12	Automated/performance/security testing
Security Engineers	3–5	Cryptography, HSM, threat modeling
Product Managers	2–3	Digital Euro requirements, roadmap
Project Manager	1	Program coordination, stakeholder mgmt
Total	**36–52**	**Full-time commitment for 3–4 years**

Development Timeline (Phased):

[leftmargin=1.5cm]

Phase 1: Foundation (Months 1–6) Architecture design, stack finalization, core API, DB schema, DevOps.

Phase 2: Core Services (Months 7–18) Access, Liquidity, Transaction, Risk frameworks, DESP integration.

Phase 3: Enhancement & Integration (Months 19–30) Offline, conditional payments, full channel integration, performance, security.

Phase 4: Testing & Readiness (Months 31–36) Unit/integration/load testing, pen tests, regulatory validation, runbooks.

Phase 5: Pilot & Production (Months 37–48) Pilot deployments, monitoring/tuning, full rollout.

5.1.4 Cost and Resource Implications

Development Costs (4-Year Period):

Cost Category	Low Estimate	High Estimate
Personnel (36–52 FTEs @ €100–150k avg)	€14.4M	€31.2M
Infrastructure (cloud, HSM, hardware)	€2M	€5M
Third-party software/licenses	€1M	€3M
Training and professional development	€0.5M	€1.5M
Testing and QA	€2M	€4M
Contingency (10–15%)	€2M	€4.5M
Total	**€21.9M**	**€49.2M**

Operational Costs (Post-Launch):

- Infrastructure and hosting: €0.5M–1M annually
- Personnel maintenance team: 8–12 FTEs (€1–1.8M annually)
- Vendor licenses and support: €0.3–0.5M annually
- **Total annual operating costs: €1.8–3.3M**

Capital Requirements:

- Upfront development: €20–50M
- Hardware and infrastructure: €5–10M
- Working capital and contingency: €5–10M
- **Total capital requirement: €30–70M**

5.1.5 Risk Profile and Mitigation Strategies

Mitigation Strategies (selected):

1. External architect review (quarterly).
2. Vendor partnerships for specialised components.
3. Pilot program before full rollout.
4. Third-party security assessments at milestones.
5. Dedicated regulatory liaison.
6. 20–25% schedule contingency and budget reserve.

5.2 Vendor/Outsourced Implementation Model

5.2.1 Model Characteristics and Applicability

Ideal Bank Profile:

- Smaller to mid-sized banks (€10–150 billion assets)
- Limited internal IT development capacity
- Existing relationships with technology vendors
- Focus on core banking rather than technology differentiation
- Lower capital availability; preference for faster time-to-market

Key Characteristics:

- Reliance on third-party vendor platforms and services
- Vendor provides integration APIs, compliance frameworks, ops support
- Bank responsibility limited to configuration, testing, distribution
- Reduced internal complexity; limited customization

5.2.2 Vendor Ecosystem and Service Models

Vendor Categories (examples):

- **Pan-European Platform Providers:** Worldline, Nexi, equensWorldline — SaaS/hosted platforms, payment processing and DESP connectivity.
- **National Champions:** SIBS (Portugal), Redsys (Spain), CBI (Italy) — domestic providers with strong local coverage.

Service Model Options:

Full-Service Platform Model Vendor provides complete solution; bank configures and distributes.

Components Outsourcing Model Bank outsources specific components (e.g., liquidity).

API Gateway Outsourcing Model Vendor manages DESP connectivity; bank develops services on top.

5.2.3 Vendor Selection and Evaluation Framework

Critical Selection Criteria:

1. Technical capabilities: schema compatibility, API completeness, performance, offline/conditional payment support.
2. Financial terms: implementation, licensing, per-transaction fees.
3. Operational support: 24/7 support, SLAs, patch cycles.
4. Regulatory and compliance: certifications, GDPR, audit trails.
5. Strategic fit: vendor stability, roadmap, vertical expertise.

Vendor Selection Process (stages):

1. Market scan & initial screening (2–3 weeks): shortlist 3–4 vendors.
2. Detailed assessment (4–6 weeks): architecture reviews, references, financials.
3. Proof of concept (4–8 weeks): prototype, integration, testing.
4. Vendor selection & negotiation (2–4 weeks): contracts, SLAs.
5. Implementation planning (4–6 weeks): detailed plan, resources.

5.2.4 Implementation Timeline and Phases

Typical Outsourced Timeline: 18–24 months

Phase 1: Platform Setup & Configuration (Months 1–4) Provisioning, configuration, env setup, initial testing.

Phase 2: Integration & Testing (Months 5–12) Core integration, API testing, channel integration, regulatory testing.

Phase 3: Pilot Deployment (Months 13–18) Limited pilot (5k–10k users), monitoring, refinement.

Phase 4: Production Rollout (Months 19–24) Gradual activation, monitoring, channel expansion.

6 Implementation Models by Bank Tier: Tailored Strategies

6.1 High-Tier Banks (Large, Internationally Active)

6.1.1 Bank Profile and Strategic Context

Typical Characteristics:

- Total assets: €300 billion to >€3 trillion
- Geographic reach: multiple countries, significant international presence
- Customer base: large retail and substantial corporate/wholesale operations
- IT infrastructure: advanced, decentralized across multiple jurisdictions
- Competitive position: market leaders with significant technical capabilities
- Strategic objectives: maintain market leadership, drive innovation, maximize shareholder value

Digital Euro Strategic Imperatives:

1. Market leadership: be among first movers with sophisticated Digital Euro services.
2. Competitive differentiation: leverage advanced capabilities for market advantage.
3. Operational integration: minimise disruption to existing operations while adding new capabilities.
4. Global coordination: manage implementation across multiple jurisdictions and banking entities.
5. Innovation positioning: position as technology innovator, not follower.

6.1.2 Recommended Implementation Approach: In-House with Selective Partnerships

Core Strategy: Develop a comprehensive in-house Digital Euro platform, utilise selective partnerships for specialised components (e.g. offline, fraud detection), create an innovation centre for next-generation features, and establish the Digital Euro as a competitive differentiator.

Detailed Implementation Architecture: Tier 1: Core Development (In-House) — Core platform components:

- Access Management Service
- Liquidity Management Service
- Transaction Management Service
- Risk and Compliance Service
- Offline Management Service
- Advanced Fraud Detection

Technical Approach:

- Microservices architecture enabling independent scaling and updates
- Distributed systems design for resilience across geographies
- Cloud-native deployment for flexibility and scalability
- Event-driven architecture for real-time processing

Tier 2: Channel Integration (In-House + Partnerships) — Distribution channels and elements:

- Mobile banking
  - Native iOS/Android apps
  - Digital Euro wallet UI
  - Offline capability support
  - Biometric authentication
- Web banking
  - Enhanced web interfaces
  - Corporate treasury portal
  - Merchant acceptance tools
- POS & Merchant
  - Terminal integration framework
  - Merchant onboarding

    - Acceptance network development
- ATM network
    - NFC upgrade support
    - QR code capability
    - Funding/defunding operations

Tier 3: Advanced Services (In-House Development) — Proprietary innovation services:

- Conditional payments engine (escrow, supply-chain financing, treasury orchestration)
- Loyalty & rewards integration (automatic point allocation, merchant incentive programs)
- Advanced analytics (real-time transaction analytics, fraud pattern detection)
- API economy for partners (developer ecosystem, fintech partnerships)
- Blockchain integration (future): smart contract compatibility and advanced programmability

6.1.3 Governance and Organizational Structure

Organizational Design (example teams and sizing):

- Chief Technology Officer (CTO)
    - Head, Digital Euro Platform
        - Platform Architecture Team (5)
        - Core Services Development (30)
            - Access & Onboarding (8)
            - Liquidity & Settlement (8)
            - Transaction Processing (8)
            - Risk & Compliance (6)
        - DevOps & Infrastructure (8)
        - Security & Privacy (5)

        - QA & Testing (10)
    - Head, Digital Euro Channels
        - Mobile Banking Enhancement (12)
        - Web & Corporate (8)
        - POS & Merchant Integration (6)
        - ATM Integration (5)
        - Quality Assurance (8)
    - Head, Digital Euro Innovation
        - Advanced Payments Team (6)
        - Analytics & Data Science (6)
        - Partner Ecosystem (4)
        - Research & Development (4)
- Chief Risk Officer (CRO)
    - Head, Digital Euro Compliance
        - Regulatory Affairs (3)
        - AML/KYC Compliance (3)
        - Risk Management (3)
        - Internal Audit (2)

Program Governance:

- Digital Euro Steering Committee (Executive Board, CTO, CFO, CRO, Chief Commercial Officer)
- Technical Architecture Review Board (monthly)
- Regulatory & Compliance Review (bi-weekly)
- Product & Innovation Council (monthly)
- External Advisory Board (quarterly) including ECB, industry experts, fintech partners

6.1.4 Cost and Timeline for High-Tier Banks

Financial Investment (48-month period):

Category	Low	High
Personnel (50+ FTEs @ €120k–150k avg)	€24M	€30M
Infrastructure (cloud, data centres, security)	€8M	€12M
Technology licenses & third-party services	€3M	€5M
External consulting & specialised expertise	€4M	€6M
Testing, QA, security	€4M	€6M
Contingency (15%)	€5.1M	€7.65M
Total Development Cost	**€48.1M**	**€66.65M**

Ongoing Annual Operating Costs (indicative):

- Personnel (12–18 FTEs): €1.5M–2.7M
- Infrastructure and hosting: €1M–2M
- Third-party services and licences: €0.5M–1M
- **Total annual: €3M–5.7M**

Timeline (high-level by year):

- Year 1 (Q1–Q4): Architecture & foundation — technology selection, DevOps setup, core framework, recruit (75% staffing).
- Year 2 (Q1–Q4): Core services development — access, liquidity, transaction services, DESP integration, internal beta.
- Year 3 (Q1–Q4): Enhancement & channel integration — risk, offline, mobile/web/POS integration, pilot (5k–10k external users).
- Year 4 (Q1–Q4): Advanced features & production — conditional payments, analytics, full channel rollout, go-live preparation.

Key milestones (examples):

- Month 6: architecture approved, core development begun.

- Month 12: core platform functional, internal testing.
- Month 24: beta pilot launched, ∼5,000 active users.
- Month 36: production launch.
- Month 48: full feature deployment, ecosystem maturity.

6.2 Mid-Tier Banks (Regional, Moderate Complexity)

6.2.1 Bank Profile and Strategic Context

Typical Characteristics:

- Total assets: €50–300 billion
- Geographic reach: primary country plus selected neighbouring markets
- Customer base: significant retail, regional corporate focus
- IT infrastructure: moderate maturity, some legacy systems
- Competitive position: regional leaders in key markets
- Strategic objectives: maintain competitive relevance, manage costs efficiently

Digital Euro Strategic Imperatives:

1. Compliance requirement: meet ECB mandates without overinvestment.
2. Cost efficiency: manage costs while maintaining quality.
3. Time-to-market: launch Digital Euro services quickly.
4. Operational integration: minimise disruption.
5. Selective differentiation: focus innovation on high-value segments.

6.2.2 Recommended Implementation Approach: Hybrid Model

Core Strategy: Outsource core integration via a vendor platform, develop selective proprietary services for regional differentiation, leverage vendor expertise while controlling costs, and achieve faster time-to-market.

Detailed Implementation Architecture: Tier 1: Vendor-Managed Core (approx. 60% effort) — Platform components (vendor responsibility):

- Access management (onboarding, KYC, wallet provisioning)
- Liquidity management (DCA operations, waterfall)
- Basic transaction processing
- Compliance framework (rulebook requirements)
- Standard reporting and statement engine

Vendor selection criteria (high level):

- Strong presence in bank's primary market and proven track record
- Comprehensive Digital Euro platform and responsive support
- Reasonable pricing aligned to bank scale

Tier 2: Shared Infrastructure (approx. 25% effort) — Market-based collaboration:

- Shared liquidity management (cooperative funding)
- Shared fraud detection consortium
- Shared ATM network operations
- Shared settlement operations
- Industry shared testing infrastructure

Tier 3: Bank-Developed Differentiation (approx. 15% effort) — Proprietary services:

- Regional payment integration and local merchant ecosystem
- SME/corporate offerings (supply chain financing, working capital)
- Enhanced customer experience (personalised merchant offers)
- Data & analytics (dashboards, competitive insights)

6.2.3 Governance and Organizational Structure

Organizational Design (example):

- Chief Information Officer (CIO)

  - Head, Digital Euro Program (1.0 FTE)
    - Program Manager (1.0 FTE)
    - Systems Integration Manager (1.0 FTE)
    - QA Lead (1.0 FTE)
    - Operations Manager (0.5 FTE)
    - Vendor Relationship Manager (0.5 FTE)
  - Head, Digital Euro Innovation (0.5 FTE)
    - Product Manager (0.5 FTE)
    - Developer (2 FTE shared)
    - Analyst (1 FTE shared)
- Chief Risk Officer (CRO): Digital Euro Compliance Officer (1.0 FTE), Regulatory Liaison (0.5 FTE), AML/KYC Manager (1.0 FTE)
- Chief Commercial Officer (CCO): Digital Euro Product Manager (1.0 FTE), Marketing Manager (0.5 FTE shared), Customer Success Manager (1.0 FTE)

Program Governance:

- Steering Committee (quarterly): CIO, CFO, CRO, CCO
- Vendor Management Review (monthly)
- Compliance & Regulatory Review (monthly)
- Product & Customer Review (bi-monthly)

6.2.4 Cost and Timeline for Mid-Tier Banks

Financial Investment (30-month period):

Category	Typical Range
Vendor platform & services	€5M–8M
Bank project management & integration	€1.5M–2.5M
In-house development (proprietary)	€3M–5M
Testing, training, change management	€1.5M–2.5M
Infrastructure and operational setup	€1M–1.5M
Contingency (15%)	€1.95M–3.15M
Total Development Cost	**€13.95M–22.65M**

Ongoing Annual Operating Costs (indicative):

- Vendor licensing/support: €1M–1.5M
- Bank operations team (3–4 FTEs): €0.4M–0.6M
- Development and enhancement (part-time): €0.3M–0.5M
- **Total annual: €1.7M–2.6M**

Timeline (high-level):

- Months 1–4: Vendor selection & planning.
- Months 5–12: Core integration phase; limited pilot (500–1,000 users).
- Months 13–18: Enhancement development and expanded pilot (2,000–5,000 users).
- Months 19–24: Production preparation and regulatory testing.
- Months 25–30: Production launch and scaling.

Key milestones (examples):

- Month 3: vendor selected and contracted.
- Month 6: platform setup complete.
- Month 12: pilot launched with ∼1,000 users.
- Month 24: production ready.
- Month 30: full customer activation.

6.3 Low-Tier Banks (Small, Community-Focused)

6.3.1 Bank Profile and Strategic Context

Typical Characteristics:

- Total assets: €5–50 billion
- Geographic reach: single country, often single region
- Customer base: retail-focused, limited corporate services
- IT infrastructure: basic systems, limited IT staff
- Competitive position: niche players in local markets
- Strategic objectives: remain compliant while managing tight budgets

Digital Euro Strategic Imperatives:

1. Cost minimisation: implement Digital Euro with minimal investment.
2. Regulatory compliance: meet ECB requirements without differentiation.
3. Resource constraints: manage with existing small IT team.
4. Time-to-market: achieve timeline without overextension.
5. Stability: avoid operational disruption to core banking.

6.3.2 Recommended Implementation Approach: Vendor/Outsourced Model

Core Strategy: Engage an established vendor for an end-to-end Digital Euro platform, minimise internal development and complexity, rely on vendor expertise and support, and focus bank resources on core banking ops.

Detailed Implementation Architecture: Vendor platform (approx. 90% of services) — typical vendor-provided services:

- Access management (onboarding, KYC, wallet management)
- Liquidity management (DCA operations, waterfall automation)
- Transaction processing (full lifecycle)
- Risk & compliance (fraud detection, AML screening)

- Channel integration (mobile, web, ATM support)
- Reporting and reconciliation
- Customer support framework and operational monitoring

Bank-specific configuration (approx. 10% effort):

- Brand integration, customer communications, regulatory documentation
- Staff training materials and customer support scripts

Vendor relationship options:

- Single vendor relationship: simplest, lowest internal overhead, but vendor dependency (typical vendors: Temenos, SAP, Oracle).
- Cooperative/consortium model: multiple banks share vendor platform, governance and costs shared (examples: Atruvia, Redsys).

6.3.3 Governance and Organizational Structure

Streamlined organisation (example):

- Chief Information Officer (CIO)
  - Digital Euro Project Manager (1.0 FTE)
  - Vendor Relationship Manager (0.5 FTE)
  - Systems Administrator (0.5 FTE shared)
  - Compliance Liaison (0.25 FTE shared)
- Chief Risk Officer (CRO)
  - Compliance Officer (0.5 FTE shared)
  - Regulatory Liaison (0.25 FTE)
- Chief Commercial Officer (CCO)
  - Product Manager (0.25 FTE shared)

Governance structure:

- Steering Committee (quarterly): CIO, CFO, CRO, CCO

- Vendor Review Meeting (monthly)
- Regulatory Check-in (monthly)

6.3.4 Cost and Timeline for Low-Tier Banks

Financial Investment (24-month period):

Category	Amount
Vendor platform implementation	€2.5M–4M
Project management and coordination	€0.4M–0.6M
Integration and configuration	€0.3M–0.5M
Testing and training	€0.3M–0.5M
Infrastructure (servers, security)	€0.3M–0.5M
Contingency (10%)	€0.38M–0.61M
Total Development Cost	**€4.18M–6.71M**

Ongoing Annual Operating Costs (indicative):

- Vendor platform licensing: €0.6M–1M
- Operational staff (1 FTE): €70k–100k
- Support and maintenance: €100k–200k
- **Total annual: €0.77M–1.3M**

Timeline (high-level):

- Months 1–3: vendor selection & planning.
- Months 4–9: implementation, configuration, pilot (1k–2k users).
- Months 10–18: integration, regulatory testing, production preparation.
- Months 19–24: production launch, staged activation and monitoring.

6.3.5 Risk Considerations and Mitigation

Primary risks and mitigations (summary):

- Complete vendor dependency — mitigation: cooperative arrangement, exit clauses.
- Limited customization — mitigation: accept standard platform features where feasible.
- Operational disruption — mitigation: thorough testing, vendor support, phased rollout.
- Data security/privacy — mitigation: vendor security certifications, regular audits.
- Cost overruns — mitigation: fixed-price contracts, scope control.

Recommended mitigation strategies:

1. Join cooperative arrangements or consortiums to reduce individual dependency and cost.
2. Establish clear SLAs with performance and support guarantees.
3. Use a phased implementation approach to manage risk and cost.
4. Provide comprehensive staff training prior to go-live.
5. Keep competent authority/regulatory oversight of the vendor relationship.

7 Shared Infrastructure, Synergies, and Cost Mutualization

8 Technical Blueprints and Best Practices

9 Regulatory Considerations and Compliance Framework

10 Conclusion and Recommendations

Appendix