Implementation Models for Banks in the Context of the Digital Euro: A Comprehensive Technical and Strategic Analysis

Author's Research Thesis

December 2025

Executive Summary

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—from €18 billion to €4-5.77 billion for the euro area banking sector—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.

1.1.1 The Strategic Context

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
- 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

- How should banks map internal data models and systems to Digital Euro Service Platform requirements?
- What are the technical implications of different API protocols (REST vs. gRPC) and architectural patterns (microservices vs. monolithic)?
- How do conditional payments and offline synchronization affect back-end design decisions?

RQ2: Implementation Models

- What are the comparative advantages and disadvantages of In-house, Hybrid, and Outsourced implementation approaches?
- How do implementation costs, timelines, and risk profiles differ across these models?
- Which implementation model is optimal for each bank tier?

RQ3: Shared Infrastructure and Mutualization

- What cost synergies can be achieved through shared infrastructure and collaborative vendor engagement?
- How do market-specific factors (vendor concentration, outsourcing prevalence, collaboration history) influence synergy potential?
- What organizational and contractual arrangements facilitate effective cost mutualization?

RQ4: Risk and Feasibility

- What are the primary technical, operational, and financial risks in Digital Euro integration?
- How can banks effectively manage the complex interplay between mandatory compliance and optional innovation?
- What governance structures and expertise requirements are necessary for successful implementation?

1.4 Research Scope and Methodology

Scope:

- Temporal focus: ECB preparation phase (2023-2025) and anticipated implementation phase (2025-2029)
- Geographic scope: Euro area banking systems across 20 euro area countries
- Bank coverage: All retail banks with significant customer bases, differentiated by asset size and market position
- Technical scope: Back-end integration, core system modifications, API implementation, and compliance infrastructure (excludes front-end user interfaces and macroeconomic impact analysis)

Methodology:
This research employs a mixed-methods approach combining:

1. **Document Analysis**: ECB rulebooks, technical specifications, progress reports, and regulatory frameworks
2. **Cost Study Synthesis**: Integration of PwC Digital Euro Cost Study, ECB cost assessment analysis, and banking association estimates
3. **Technical Modeling**: Analysis of functional architectures, API specifications, and data flow diagrams
4. **Comparative Case Analysis**: Examination of implementation approaches across different banking models and geographies
5. **Synergy Assessment**: Quantitative evaluation of mutualization opportunities using structured vendor and outsourcing analysis
6. **Scenario Analysis**: Development of cost and complexity projections across three implementation model scenarios

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:

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

Functional Roles:

The Digital Euro serves multiple complementary functions within the European payment ecosystem:

1. **Store of Value**: Users can hold Digital Euro balances (subject to holding limits protecting financial stability)

2. **Medium of Exchange**: Enables seamless peer-to-peer, point-of-sale, and e-commerce transactions
3. **Unit of Account**: Denominated in euros, maintaining direct parity with physical cash
4. **Payment Resilience**: Offline functionality provides transaction capability during network outages
5. **Financial Inclusion**: Accessible to all euro area residents without traditional banking relationships

2.1.2 Key Digital Euro Ecosystem Actors

The Digital Euro ecosystem comprises several interconnected participant categories:

Eurosystem (ECB and National Central Banks)

- 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 for offline solutions
- Security and encryption service providers
- Payment terminal manufacturers

2.2 The Eurosystem's Digital Euro Project Evolution

2.2.1 Project Phases and Timeline

Investigation Phase (October 2021 - October 2023): Design Exploration

Objectives:

- Establish conceptual design for Digital Euro
- Explore distribution models and PSP roles
- Develop functional and non-functional requirements
- Create stakeholder engagement platforms

Outputs:

- High-level digital euro product design
- User requirements specifications
- Digital Euro Report (October 2020) and subsequent stocktake documents
- Euro Retail Payments Board (ERPB) engagement framework

Preparation Phase (November 2023 - October 2025): Operational Readiness

Objectives:

- Develop comprehensive draft Digital Euro Scheme Rulebook
- Select technology providers and platform operators
- Conduct experimentation through innovation platforms
- Perform technical validation and feasibility studies
- Deepen market and legislative engagement

Key Achievements:

- Rulebook version evolution (0.8a → 0.9 draft)
- Selection of 5 external providers and 6 Eurosystem entities for DESP components
- Innovation Platform engagement (~70 market participants)
- Conditional payments technical validation
- Offline functionality design and secure element analysis
- User research across vulnerable populations and small merchants
- Financial stability analysis and holding limit calibration methodology
- Cost assessment studies and synergy analysis frameworks

Implementation Phase (2025-2029): Build and Deploy

Planned Activities (subject to legislation approval):

- Technical capacity building and development
- Pilot testing and validation (potential start: mid-2027)
- Market readiness programs and compliance certification
- Phased functionality roll-out
- Possible first issuance (2029 target)

2.3 Structural Components of the Digital Euro Infrastructure

2.3.1 Digital Euro Service Platform (DESP) Architecture

The DESP represents the technical core of the Digital Euro infrastructure, providing centralized settlement and clearing functions while enabling distributed processing across PSPs and Eurosystem components. The architecture embodies several key design principles:

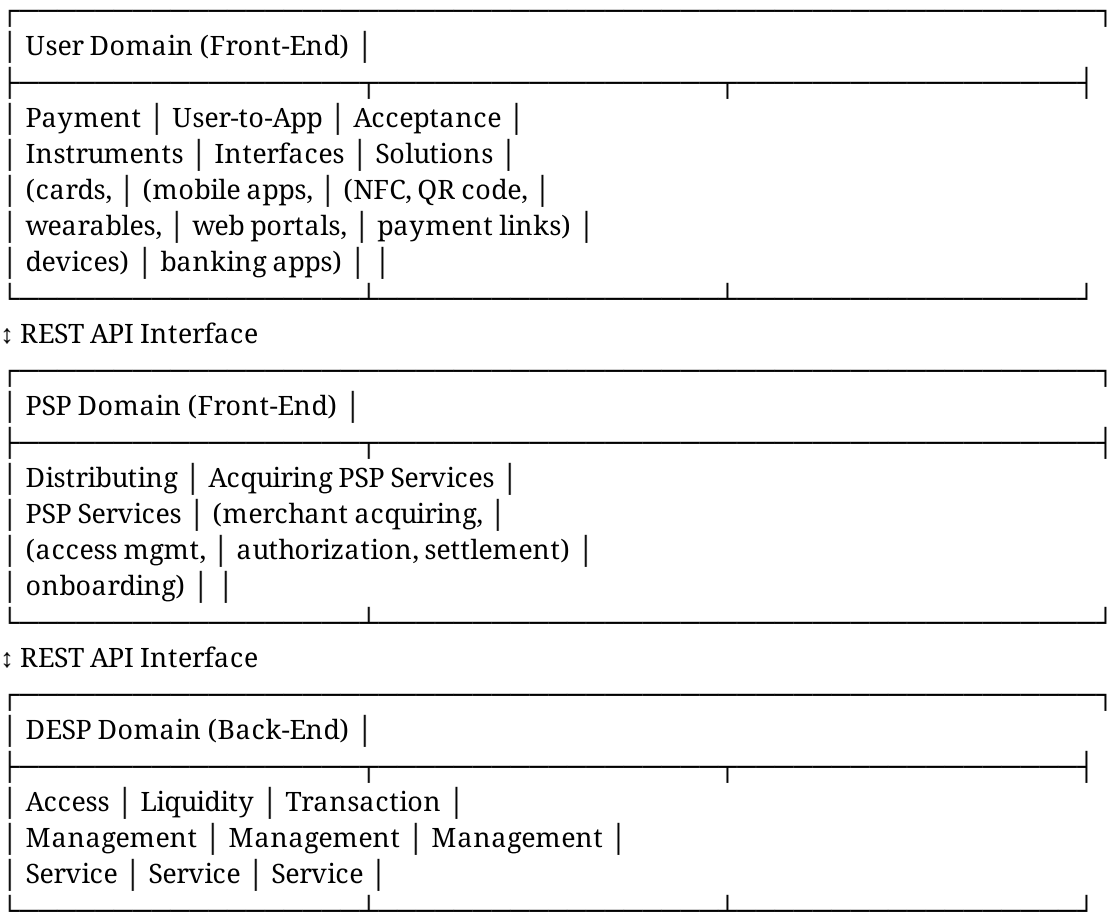
Multi-Region Resilience:

- Centralized ledger maintaining authoritative transaction records
- Multi-region deployment across three geographic regions
- Multiple servers and data centers per region
- Automatic failover and regional disaster recovery
- Ensures continuity even if entire regional infrastructure fails

Privacy-Preserving Design:

- End-user identities unknown to the Eurosystem
- PSPs perform KYC/AML functions and onboarding
- Transactions processed using pseudonymous identifiers
- Segregated, distributed processing across DESP components
- No transaction linking to individuals by central bank

Functional Domains (three-layer architecture):



Core Components:

1. **Access Management Service**: Manages onboarding, offboarding, wallet provisioning, and user authentication
2. **Liquidity Management Service**: Handles funding/defunding operations via Dedicated Cash Accounts (DCAs), waterfall mechanisms
3. **Transaction Management Service**: Processes payment instruction, clearing, and settlement
4. **Settlement Layer**: Maintains ledger, executes final settlement, ensures atomicity
5. **Conditionality Layer**: Enables conditional payments through fund reservation mechanisms
6. **Offline Management**: Handles secure element provisioning and offline transaction reconciliation

2.3.2 Dedicated Cash Accounts (DCAs) and Liquidity Management

DCAs represent a critical mechanism bridging PSPs' operational needs with the DESP's settlement requirements:

DCA Functions:

- Individual account held by each PSP at respective National Central Bank (NCB)
- Provides liquidity source for funding Digital Euro customer holdings
- Enables efficient settlement and collateral management
- Supports waterfall mechanism: funds flow from PSP DCA → Digital Euro accounts → user wallets

Operational Mechanics:

PSP Treasury/Liquidity
↓
[DCA at NCB]
↓
PSP's Digital Euro Distribution Account
↓
Individual Customer Digital Euro Wallets
↓
Transaction Settlement

Reverse Waterfall (Customer Preference):

- Users can link Digital Euro wallets directly to commercial bank accounts
- Enables large payments without pre-funding
- Maintains user convenience while managing holding limits
- Reduces liquidity burden on PSPs

2.3.3 Advanced Digital Euro Features and Functionalities

Conditional Payments:

Conditional payments enable automated fund release upon satisfaction of predefined conditions, with applications across multiple use cases:

- **E-Commerce**: Funds held in reservation until merchant confirms delivery
- **Subscription Services**: Automatic periodic payments subject to service continuation
- **Buy Now, Pay Later**: Installment payments triggered by scheduled dates
- **Service Delivery Confirmation**: Public transport, courier services with delivery confirmation
- **Escrow-like Functions**: Multi-party conditional transactions

Technical Implementation:

- Fund reservation functionality maintains reserved amounts distinct from available balance
- Conditionality layer (developed by market participants) monitors condition triggers
- Settlement layer (Eurosystem) executes fund transfer upon condition verification
- Timeout mechanisms return unreleased funds to payer after expiration

Offline Functionality:

Offline capability represents a key innovation ensuring payment resilience in network-compromised scenarios:

Design Characteristics:

- Bearer-like instrument: funds stored in secure element, ownership defined by possession
- Privacy preservation: no record sent to PSP or Eurosystem during offline payment
- Device-to-device transactions: near-field communication (NFC) between devices
- Secure elements: eSIM, embedded secure elements (eSE), or integrated secure enclaves
- Automatic reconciliation: upon reconnection, balances reconciled with DESP

Use Cases:

- Areas with limited connectivity (rural regions, remote locations)
- Emergency scenarios: power outages, network failures
- Financial resilience: continued payment functionality during infrastructure disruptions
- Enhanced privacy: transactions without transaction record linkage

Secure Element Technologies:

1. **eSIM (Embedded SIM)**: Growing market adoption, software-updatable, strong connectivity integration
2. **Embedded Secure Element (eSE)**: Tamper-resistant chip, higher security level, physical integration requirement
3. **Integrated Secure Enclaves**: Tamper-resistant hardware within device, cost-efficient for device manufacturers

2.4 Rulebook Development: Standards and Governance

The Digital Euro Scheme Rulebook establishes a single set of rules, standards, and procedures applicable across all PSPs and users in the euro area, ensuring consistent service delivery and user experience.

2.4.1 Rulebook Structure and Development Process

Development Methodology:

- Collaborative, iterative process with Rulebook Development Group (RDG)
- Market consultation incorporating PSP feedback (2,000+ unique comments in 2024 review)
- Dedicated RDG workstreams addressing implementation specifications, user experience, risk management
- Phased approach reflecting ECB design decisions and legislative developments

Rulebook Components:

1. **Functional and Operational Model**
    - Scope of basic services and use cases
    - Roles and responsibilities of each ecosystem participant

    - User journeys and end-to-end process flows
2. **Technical Requirements**
    - API specifications and integration standards
    - Data models and interchange formats
    - Security and cryptographic requirements
    - Non-functional requirements (latency, availability, throughput)
3. **User Experience Standards**
    - Minimum UX requirements for consistency across PSPs
    - Authentication, notification, and information display standards
    - Accessibility requirements for inclusive access
    - Optional enhancements supporting innovation
4. **Compliance and Risk Management**
    - Fraud detection and prevention mechanisms
    - Dispute resolution procedures
    - Anti-money laundering and know-your-customer requirements
    - Operational resilience standards
5. **Certification and Adherence Framework**
    - Testing protocols and certification requirements
    - Device and application approval processes
    - Compliance verification mechanisms
    - Onboarding process for new PSPs
6. **Brand Rules and User Protections**
    - Consistent Digital Euro brand application
    - Logo usage guidelines
    - Dispute management procedures
    - User rights and protections

2.4.2 Implementation Specifications

Implementation specifications translate rulebook requirements into operational details for PSP developers:

Front-End Implementation Specifications:

- End-user device interfaces (mobile, wearable, card)
- Acceptance solution specifications (NFC, QR code, payment links)
- User journey process flows and decision trees
- Integration with existing PSP applications
- Supported standards: CPACE, EPC standards, nexo, Berlin Group protocols

Back-End Implementation Specifications:

- PSP-to-DESP API interfaces and protocols
- Settlement service specifications
- Alias lookup and account identification
- Liquidity management and DCA operations
- Transaction processing workflows
- Offline reconciliation procedures

---

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)

Context: Largest retail CBDC deployment, initiated 2014, pilot phase initiated 2020

Key Technical Features:

- Two-tier system: central bank (issuance) and commercial banks/PSPs (distribution)
- Offline capability through hardware wallets and secure elements
- Programmable money with smart contract integration
- Real-time gross settlement

Lessons for Digital Euro:

- Two-tier PSP engagement model validates distribution approach
- Offline functionality complexity requires long development and testing cycles
- Hardware integration challenges (device manufacturers, security requirements)
- User adoption highly dependent on merchant acceptance incentives

Implementation Scale:

- ~300 million transaction pilots as of 2024
- Deployment across 23 cities
- Integration with retail merchant infrastructure

Bahamas Sand Dollar

Context: First retail CBDC launch (2020), population ~400,000

Key Technical Features:

- Digital wallet provisioning for unbanked populations
- Mobile-first design
- Integration with existing payment infrastructure

Lessons for Digital Euro:

- Financial inclusion design essential from inception
- Mobile-first approach reduces infrastructure dependency
- Smaller scale enables more controlled feature roll-out
- User authentication and fraud prevention critical for public trust

Sweden e-Krona Pilot

Context: Extended pilot (2020-2024), focus on offline functionality and retail adoption

Key Technical Features:

- Emphasis on offline payment mechanisms
- Integration with existing electronic payment systems
- Focus on edge cases (rural areas, elderly population)

Lessons for Digital Euro:

- Offline functionality testing requires comprehensive scenario coverage
- User testing with vulnerable populations identifies accessibility issues
- Merchant integration more complex than consumer adoption
- Long pilot periods (3+ years) enable iterative improvement

3.2 Technical Standards and Best Practices

3.2.1 Payment Industry Standards Applicable to Digital Euro

The Digital Euro design leverages established standards from the payments industry, reducing integration complexity and enabling interoperability:

ISO 20022 - Payment Message Standards

- Universal standard for payment transaction information exchange
- Supports structured, machine-readable formats
- Enables integration with existing SEPA infrastructure
- Rulebook mandates ISO 20022 compliance for transaction messaging

PSD2 (Payment Services Directive 2) Alignment

- REST API interfaces built on PSD2 implementation experience
- Provides familiar integration patterns for PSPs
- Reduces learning curves and implementation timelines
- Leverages existing PSP technical infrastructure

SEPA (Single Euro Payments Area) Infrastructure

- Digital Euro complements rather than replaces SEPA
- Leverages SEPA instant credit transfer (SCTInst) experience
- Uses similar participant frameworks and governance
- Enables seamless A2A (account-to-account) integration

Open Standards for Front-End Processing

- CPACE: Contactless card payment standard
- EPC standards: QR code payments (EPC024-22), SEPA Request-to-Pay
- nexo: Balance updates and ATM transactions
- Berlin Group: Mobile P2P and open finance APIs

3.2.2 Cybersecurity and Privacy Standards

GDPR Compliance

- Pseudonymization of transaction data
- Data minimization: only necessary personal data captured
- User control over personal information
- Privacy by design principles embedded in architecture

Privacy-Enhancing Technologies

- Zero-knowledge proofs for offline transactions
- Blind signatures and cryptographic obscuration
- Segregated data processing preventing identity linkage
- Cryptographically secure token transfers

Cybersecurity Standards

- Common Criteria (CC) EAL4 or higher for secure elements
- TLS 1.3+ for communications encryption
- Hardware security modules (HSM) for cryptographic key management
- Regular security testing and penetration assessments

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:

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

Cost Distribution by Service Bundle:

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:

- Excludes offline functionality (requirements not sufficiently detailed)
- Excludes multiple account functionality
- Based on rulebook v0.8a (evolution to v0.9 may modify costs)
- 46% of available skilled resources tied up per year for 4 years

ECB Assessment of Digital Euro Investment Costs (October 2025)

Approach: Synthesis of PwC estimates with synergy and mutualization analysis

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%)

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% market synergies, 90-98% IPS banking group synergies): €4.0-5.77 billion

- High scenario (40% 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% of senior IT staff for 3-4 years
- 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% of IT staff)
- 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% of IT staff)
- 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:
Alias Registration Request
↓
Validate user ownership of alias
↓
Submit to DESP Alias Lookup Service
↓
Maintain local mapping for rapid resolution
↓
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:
Transaction Initiation (Bank Format)
↓
Transform to ISO 20022 format
↓
Submit to DESP via REST API
↓
Parse response and update local systems

↓
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) ≠ 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

The DCA represents the critical bridge between bank liquidity management and Digital Euro distribution:

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

Integration Complexity: MEDIUM

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

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:

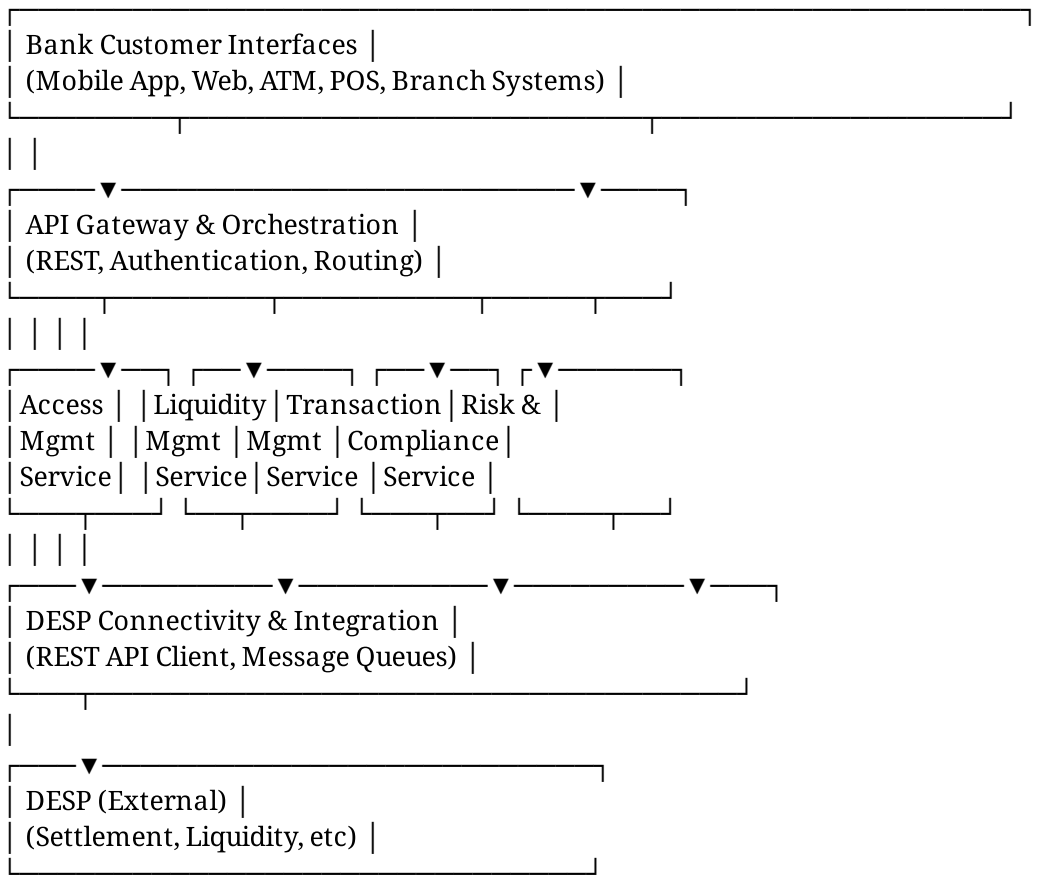
- Large, internationally active banks (typically >€300 billion assets)
- Advanced IT infrastructure and development capabilities
- Significant technical staff and specialized expertise
- Decentralized operations requiring customization
- Strategic need for competitive differentiation
- Sufficient capital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

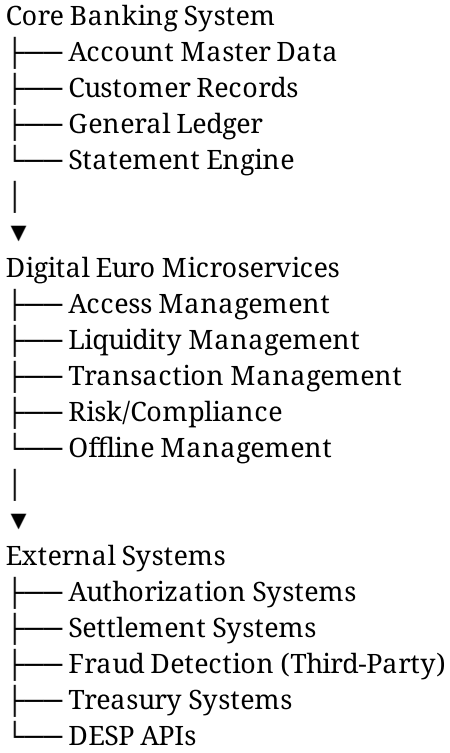


Microservices Components:

1. **Access Management Service**
   - Functions: Onboarding, wallet provisioning, alias management
   - Technology stack: Java/Spring Boot, PostgreSQL
   - API endpoints: User creation, verification, wallet activation
   - Dependencies: Core banking system, KYC/AML systems
2. **Liquidity Management Service**
   - Functions: DCA monitoring, waterfall operations, funding triggers
   - Technology stack: Node.js, MongoDB, Redis caching
   - API endpoints: DCA balance inquiry, waterfall request, reverse waterfall
   - Dependencies: Treasury systems, settlement systems, DESP
3. **Transaction Management Service**
   - Functions: Transaction processing, clearing, settlement coordination
   - Technology stack: Java, Kafka message queue, PostgreSQL
   - API endpoints: Payment instruction, authorization, clearing
   - Dependencies: Authorization systems, clearing houses, fraud detection
4. **Risk and Compliance Service**
   - Functions: Fraud detection, AML screening, risk scoring
   - Technology stack: Python (AI/ML), Apache Spark, feature store
   - API endpoints: Risk scoring, transaction flagging, compliance reporting
   - Dependencies: Regulatory reporting systems, sanctions databases

5. **Offline Management Service**
    - Functions: Secure element provisioning, offline wallet management
    - Technology stack: C++, hardware security module (HSM) integration
    - API endpoints: Secure element provisioning, offline wallet creation
    - Dependencies: Device manufacturers, secure element providers

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, infrastructure automation, monitoring
QA/Testing Engineers	8-12	Automated testing, performance testing, security testing
Security Engineers	3-5	Cryptography, secure element integration, threat modeling
Product Managers	2-3	Digital Euro requirements, market understanding, roadmap
Project Manager	1	Program coordination, stakeholder management, timeline tracking
Total	**36-52**	**Full-time commitment for 3-4 years**

Development Timeline:

Phase 1: Foundation (Months 1-6)
├── Architecture design and stakeholder review
├── Technology stack finalization
├── Core API framework development
├── Database schema and integration patterns
└── DevOps infrastructure setup

Phase 2: Core Services (Months 7-18)
├── Access Management Service
├── Liquidity Management Service
├── Transaction Management Service
├── Risk/Compliance framework
└── DESP integration framework

Phase 3: Enhancement & Integration (Months 19-30)
├── Offline Management Service
├── Advanced conditional payments
├── Full channel integration (POS, ATM, etc.)
├── Performance optimization
└── Security hardening

Phase 4: Testing & Readiness (Months 31-36)
├── Comprehensive testing (unit, integration, load)
├── Security penetration testing
├── Regulatory compliance validation
├── Go-live preparation
└── Operational runbook development

Phase 5: Pilot & Production (Months 37-48)
├── Limited pilot deployment
├── Performance monitoring and tuning
├── User feedback incorporation
└── Full production 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 quality assurance	€2M	€4M
Contingency (10-15%)	€2M	€4.5M
Total	**€21.9M**	**€49.2M**

Operational Costs (Post-Launch):

- Infrastructure and hosting: €500k-1M annually
- Personnel maintenance team: 8-12 FTEs (€1-1.8M annually)
- Vendor licenses and support: €300-500k 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

Key Risks in In-House Implementation:

Risk	Probability	Impact	Mitigation
Development delays and overruns	HIGH	HIGH	Agile methodology, external architecture review, contingency timeline
Skills gaps in emerging technologies	MEDIUM	HIGH	External consulting, vendor partnerships, training programs
Integration complexity with legacy systems	HIGH	MEDIUM	Strangler pattern, phased integration, dedicated integration team
Security vulnerabilities	MEDIUM	CRITICAL	Security review process, bug bounty programs, third-party testing
Regulatory compliance gaps	MEDIUM	HIGH	Compliance officer engagement, regulatory review checkpoints
Operational readiness issues	MEDIUM	MEDIUM	Pilot phase, comprehensive testing, operational runbook development
Resource availability	HIGH	MEDIUM	Dedicated hiring, external contractors, phased team building

Mitigation Strategies:

1. **External Architect Review**: Engage independent architecture review firm (quarterly)
2. **Vendor Partnerships**: Establish strategic partnerships with technology providers for specialized components
3. **Pilot Program**: Develop limited pilot with subset of users before full rollout
4. **Security Reviews**: Third-party security assessments at key milestones
5. **Compliance Officer**: Dedicated regulatory liaison coordinating with competent authorities
6. **Contingency Planning**: 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 for major infrastructure investments
- Preference for faster time-to-market

Key Characteristics:

- Reliance on third-party vendor platforms and services
- Vendor provides integration APIs, compliance frameworks, and operational support
- Bank responsibility limited to configuration, testing, and distribution
- Reduced internal complexity and resource requirements
- Limited customization and feature differentiation capabilities

5.2.2 Vendor Ecosystem and Service Models

Vendor Categories and Examples:

Pan-European Platform Providers:

1. **Worldline**
    - Coverage: 19 euro area countries
    - Services: End-to-end Digital Euro platform, payment processing, fraud detection
    - Model: SaaS-based platform with integration APIs
    - Customers: Medium to large PSPs
2. **Nexi**
    - Coverage: Italy, Spain, other southern European markets
    - Services: Card issuing, acquiring, Digital Euro integration
    - Model: Hosted platform with customizable components
    - Customers: Banks of various sizes in primary markets
3. **equensWorldline**
    - Coverage: Selected euro area markets
    - Services: Payment processing, Digital Euro connectivity
    - Model: Outsourced processing with integration options
    - Customers: Smaller to medium-sized banks

National Champions:

1. **SIBS (Portugal)**
    - Coverage: Portugal primarily
    - Services: Domestic payments, Digital Euro integration
    - Model: Monopoly provider for Portuguese domestic payments
    - Customers: All Portuguese banks (virtually mandatory)
2. **Redsys (Spain)**
    - Coverage: Spain
    - Services: Card processing, authentication, Digital Euro integration

    - Model: Central provider model with mandatory participation
    - Customers: All Spanish PSPs
3. **CBI (Italy)**
    - Coverage: Italy
    - Services: Interbank clearing, payments infrastructure
    - Model: Cooperative infrastructure provider
    - Customers: Italian banks and payment processors

Service Model Options:

Full-Service Platform Model:

- Vendor provides complete Digital Euro integration solution
- Bank configures platform for specific requirements
- Vendor manages DESP connectivity, compliance, updates
- Bank maintains customer relationship and distribution

Components Outsourcing Model:

- Bank outsources specific components (e.g., liquidity management)
- Vendor provides APIs for integration with bank's other systems
- Bank maintains responsibility for overall integration
- More flexibility but higher complexity

API Gateway Outsourcing Model:

- Vendor manages DESP connectivity and API gateway
- Bank develops specific services internally using vendor APIs
- Hybrid approach balancing flexibility and simplicity
- Requires internal development capability

5.2.3 Vendor Selection and Evaluation Framework

Critical Selection Criteria:

1. **Technical Capabilities**
    - Digital Euro schema compatibility
    - API completeness and documentation
    - Performance and scalability metrics
    - Support for advanced features (offline, conditional payments)
    - Integration with bank's existing systems
2. **Financial Terms**
    - Implementation fees
    - Licensing/SaaS costs
    - Per-transaction fees (if applicable)
    - Support and maintenance costs
    - Upgrade and enhancement costs
3. **Operational Support**
    - 24/7 technical support
    - SLA guarantees and penalties
    - Response time commitments
    - Regular update cycles and security patches
    - Professional services for implementation

4. **Regulatory and Compliance**
    - Regulatory approval and certifications
    - Compliance with Digital Euro rulebook
    - Data protection and GDPR compliance
    - Security certifications and assessments
    - Audit trail and reporting capabilities
5. **Strategic Fit**
    - Vendor financial stability and roadmap
    - Market positioning and customer base
    - Innovation track record
    - Vertical expertise in banking/payments
    - Growth trajectory and future capability

Vendor Selection Process:

Stage 1: Market Scan & Initial Screening (2-3 weeks)
├── Identify potential vendors (5-10 candidates)
├── Request preliminary information
├── Screen for basic capability fit
└── Short-list 3-4 vendors

Stage 2: Detailed Assessment (4-6 weeks)
├── Detailed capability presentations
├── Technical architecture reviews
├── Reference checks with existing customers
├── Financial proposal evaluation
└── Security and compliance assessment

Stage 3: Proof of Concept (4-8 weeks)
├── Technical prototype development
├── Integration with bank's test environment
├── Performance and scalability testing
├── Security assessment
└── Evaluation and comparison

Stage 4: Vendor Selection & Negotiation (2-4 weeks)
├── Final vendor selection
├── Contract negotiation
├── SLA definition
├── Support model finalization
└── Implementation planning

Stage 5: Implementation Planning (4-6 weeks)
├── Detailed project planning
├── Resource allocation
├── Timeline development
├── Risk assessment
└── Go-live preparation

5.2.4 Implementation Timeline and Phases

Typical Outsourced Implementation Timeline: 18-24 Months

Phase 1: Platform Setup & Configuration (Months 1-4)
├── Platform provisioning and access
├── System configuration for bank requirements
├── Integration environment setup
├── Compliance rule configuration
└── Initial testing

Phase 2: Integration & Testing (Months 5-12)
├── Integration with bank core systems
├── API development and testing
├── Channel integration (mobile, web, ATM)
├── Regulatory testing and certification
├── Performance and load testing

Phase 3: Pilot Deployment (Months 13-18)
├── Limited customer pilot (5,000-10,000 users)
├── Operational testing
├── Performance monitoring
├── User feedback collection
└── Refinement and optimization

Phase 4: Production Rollout (Months 19-24)
├── Gradual customer activation
├── Monitoring and support
├── Channel expansion (POS, e-commerce)
├── Feature enhancements
└── Full production operations

5.2.5 Cost and Resource Implications

Implementation Costs (Full Lifecycle):

Cost Category	Typical Range
Platform license/setup	€2M-5M
Implementation services	€1M-3M
Integration consulting	€500k-1.5M
Testing and quality assurance	€500k-1M
Training and change management	€300k-500k
Contingency (15%)	€600k-1.5M
Total Implementation Cost	**€5M-13M**

Ongoing Costs (Annual):

- Platform licensing/SaaS: €1M-2M annually
- Per-transaction fees (if applicable): Variable (€0.01-0.05 per transaction)
- Support and maintenance: €300k-600k annually
- Upgrades and enhancements: €200k-500k annually
- **Total annual operating cost: €1.5M-3.5M**

Resource Requirements:

- Project manager: 1 FTE (full implementation period)
- Systems analyst: 2-3 FTEs (implementation phase only)
- Business analyst: 2 FTEs (implementation phase)
- Compliance officer: 0.5 FTE (ongoing)
- Operations staff: 3-5 FTEs (ongoing)
- **Total dedicated staff: 8-12 FTEs during implementation, 3-6 ongoing**

5.2.6 Risk Profile and Mitigation Strategies

Key Risks in Vendor/Outsourced Model:

Risk	Probability	Impact	Mitigation
Vendor lock-in	MEDIUM	MEDIUM	Clear exit terms, API documentation, data portability clauses
Vendor financial instability	LOW	CRITICAL	Financial stability review, escrow arrangements, backup vendor relationships
Service disruptions	LOW	HIGH	SLA guarantees, redundancy requirements, support escalation procedures
Limited customization	MEDIUM	MEDIUM	Flexible API design, professional services options, vendor roadmap alignment
Integration complexity	MEDIUM	MEDIUM	Clear integration specifications, proof of concept, dedicated integration support
Regulatory compliance gaps	LOW	HIGH	Vendor certifications, compliance review process, regulatory liaison
Feature limitations	MEDIUM	LOW	Roadmap alignment, feature request processes, upgrade planning

Mitigation Strategies:

1. **Vendor Diversification**: Maintain relationships with 2+ vendors, avoid complete dependency
2. **API Standardization**: Require vendor adherence to open standards enabling future transitions
3. **Escrow Arrangements**: Place vendor code and documentation in escrow for business continuity
4. **SLA Guarantees**: Establish clear performance and uptime SLAs with financial penalties
5. **Exit Clauses**: Define clear exit provisions and data transition procedures
6. **Regulatory Oversight**: Maintain regulatory authority oversight of vendor relationship

5.3 Hybrid Implementation Model: Balanced Approach

5.3.1 Model Characteristics and Applicability

Ideal Bank Profile:

- Mid-sized to large banks (€100-500 billion assets)
- Moderate to advanced IT capabilities
- Strategic need for differentiation in selected areas
- Desire to balance cost efficiency with feature flexibility
- Multi-market operations requiring selective customization
- Interest in building Digital Euro as competitive advantage

Key Characteristics:

- Outsourced core integration with vendor platform
- Selective in-house development for high-value services
- Leverages vendor capabilities for commodity functions
- Develops proprietary value-added services
- Balanced risk and resource allocation

5.3.2 Hybrid Model Architecture

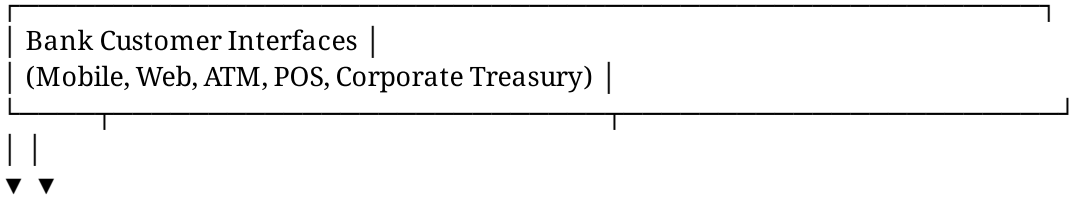
Tiered Integration Approach:

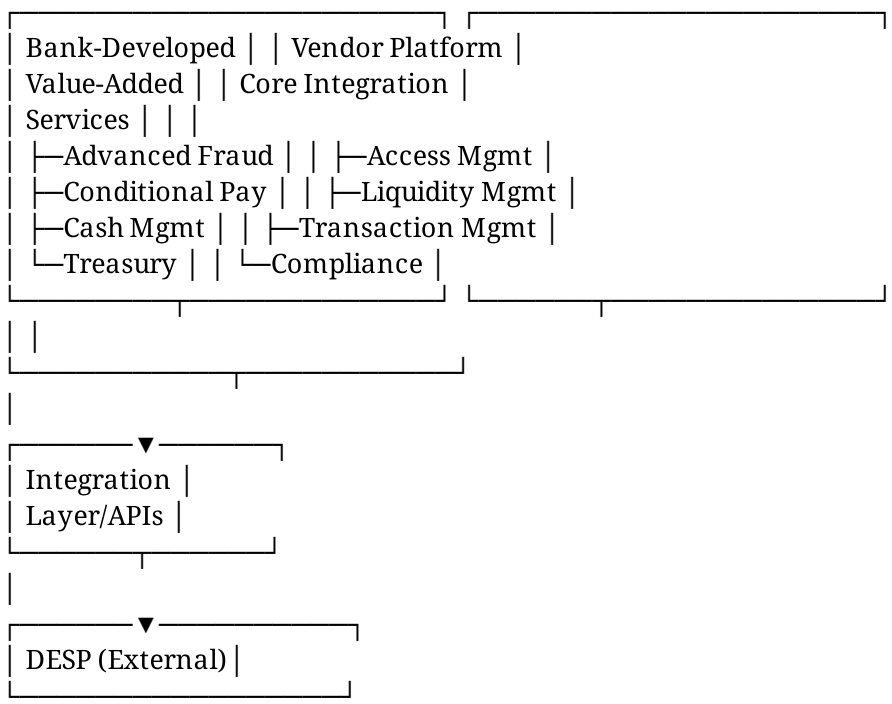
Tier 1: Outsourced Core Integration (Vendor-Managed)
├── Access Management
├── Liquidity Management
├── Basic Transaction Processing
├── Compliance Framework
└── Standard Reporting

Tier 2: Integrated Enhancements (Bank-Managed)
├── Advanced Fraud Detection
├── Conditional Payment Enhancements
├── Liquidity Forecasting
├── Customer Segmentation
└── Advanced Analytics

Tier 3: Proprietary Value-Added Services (Bank-Developed)
├── Merchant Loyalty Integration
├── Supply Chain Financing
├── Working Capital Solutions
├── Subscription/Recurring Payment Management
└── Corporate Treasury Integration

Implementation Architecture:





5.3.3 Value-Added Service Examples

Advanced Conditional Payments for B2B

- Bill pay integration with advanced scheduling
- Escrow arrangements for high-value transactions
- Installment payment management for equipment leasing
- Dynamic discounting for early payment
- Working capital optimization

Technical Implementation:

- Build on vendor's conditional payment framework
- Bank develops custom condition evaluation logic
- Integration with corporate treasury systems
- Sophisticated reporting and analytics

Merchant Loyalty and Incentive Management

- Automatic loyalty point award with Digital Euro transactions
- Targeted merchant promotions and cashback offers
- Network effects: incentivize merchant acceptance
- Consumer engagement through gamification

Technical Implementation:

- APIs for loyalty program integration
- Real-time transaction data for promotion triggering
- Reconciliation with merchant accounting systems

Liquidity and Cash Management Enhancements

- Predictive liquidity forecasting using ML

- Automated funding optimization
- Integration with FX and hedging strategies
- Real-time liquidity dashboard for treasury teams

Technical Implementation:

- Data pipeline from transaction systems to analytics platform
- Machine learning model development
- API for treasury system integration

Supply Chain Financing

- Supplier financing on Digital Euro payments
- Automated invoice discounting
- Working capital optimization across supply chains
- Integration with procurement systems

Technical Implementation:

- Supply chain data integration
- Financial modeling and pricing engines
- Integration with supplier and buyer financial systems

5.3.4 Development and Integration Approach

Phased Implementation Strategy:

Phase 1: Core Integration (Months 1-12)
├── Vendor platform setup and configuration
├── Integration with bank core systems
├── Basic compliance and reporting
├── Channel integration (mobile, web)
└── Pilot with initial customer base

Phase 2: Enhancement Development (Months 9-20)
├── Parallel development of value-added services
├── Integration design for enhancement components
├── Testing of enhancement features
├── Pilot integration with core platform
└── Performance optimization

Phase 3: Advanced Features (Months 18-30)
├── Launch first value-added service (e.g., advanced fraud)
├── Gather performance metrics and feedback
├── Develop subsequent value-added services
├── Market testing and refinement
└── Feature differentiation demonstration

Phase 4: Scaling and Optimization (Months 25-36)
├── Scale successful value-added services
├── B2B/Treasury channel expansion
├── Cross-sell and upsell program development
├── Competitive positioning and marketing
└── Long-term roadmap development

Team Structure:

Component	Team	Size	Reporting
Core Integration	Vendor + Bank Integration Team	3-5 bank staff	CIO
Advanced Fraud Development	Bank Security/Risk Team	3-4 people	Chief Risk Officer
Conditional Payments Enhancement	Bank Product Team	2-3 people	Head of Payments
Treasury Integration	Bank Treasury IT	2-3 people	Treasurer
Data/Analytics	Bank Analytics Team	2-3 people	Chief Data Officer
Overall Program	Program Manager	1 FTE	CIO/CFO

5.3.5 Cost and Resource Implications

Cost Profile (3-Year Period):

Cost Category	Amount
Vendor platform licensing & implementation	€5M-8M
Bank development (value-added services)	€8M-15M
Integration and consulting services	€2M-4M
Testing, training, and change management	€2M-3M
Contingency (15%)	€2.5M-4.5M
Total Implementation Cost	**€20M-35M**

Ongoing Operating Costs (Annual):

- Vendor licensing and support: €1.5M-2.5M
- Bank development team (5-8 people): €600k-1.2M
- Infrastructure and hosting: €300k-500k
- **Total annual cost: €2.4M-4.2M**

Resource Requirements:

- Implementation period: 20-30 FTEs for 18-24 months

- Ongoing: 6-10 FTEs for continuous development and operations
- External support: 3-5 FTEs from consulting firms for first 12 months

5.3.6 Risk Profile and Mitigation Strategies

Key Risks in Hybrid Model:

Risk	Probability	Impact	Mitigation
Integration complexity	MEDIUM	MEDIUM	Clear integration architecture, dedicated integration team
Development delays on enhancements	MEDIUM	MEDIUM	Agile methodology, experienced development leadership
Vendor/bank misalignment	MEDIUM	MEDIUM	Clear governance, steering committee, regular communication
Feature duplication and conflicts	MEDIUM	LOW	Architecture review, clear separation of concerns
Skill gaps in bank team	MEDIUM	MEDIUM	Training programs, external mentoring, phased development
Regulatory compliance complexity	LOW	MEDIUM	Compliance officer oversight, regulatory testing

Mitigation Strategies:

1. **Clear Separation of Concerns**: Well-defined boundaries between vendor platform and bank enhancements
2. **Integration Architecture Review**: Third-party review of integration approach
3. **Governance Structure**: Joint steering committee with vendor and bank leadership
4. **Agile Development**: Sprint-based development with regular demos and feedback
5. **Compliance Officer Oversight**: Dedicated compliance review at each development phase
6. **Performance Baseline**: Clear metrics for vendor platform and bank enhancements

---

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, 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**: Minimize 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 comprehensive in-house Digital Euro platform
- Utilize selective partnerships for specialized components (offline, fraud detection)
- Create innovation center for next-generation features
- Establish Digital Euro as 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:
├── 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
│ ├── Advanced escrow capabilities
│ ├── Supply chain financing
│ └── Treasury payment orchestration
├── Loyalty & Rewards Integration
│ ├── Automatic point allocation
│ ├── Merchant incentive programs
│ └── Consumer engagement features
├── Advanced Analytics
│ ├── Real-time transaction analytics
│ ├── Fraud pattern detection
│ ├── Customer behavior insights
│ └── Competitive intelligence
├── API Economy for Partners
│ ├── Developer ecosystem
│ ├── Third-party service integration
│ └── Fintech partnership framework
└── Blockchain Integration (Future)
├── Smart contract compatibility
├── Supply chain transparency
└── Advanced programmability

6.1.3 Governance and Organizational Structure

Organizational Design:

```
Chief Technology Officer (CTO)
│
├── Head, Digital Euro Platform
│   ├── Platform Architecture Team (5 people)
│   ├── Core Services Development (30 people)
│   │   ├── 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	Amount
Personnel (50+ FTEs @ €120k-150k avg)	€24M-30M
Infrastructure (cloud, data centers, security)	€8M-12M
Technology licenses and third-party services	€3M-5M
External consulting and specialized expertise	€4M-6M
Testing, quality assurance, security	€4M-6M
Contingency (15%)	€5.1M-7.65M
Total Development Cost	**€48.1M-66.65M**

Ongoing Annual Operating Costs:

- Personnel (12-18 FTEs for maintenance/enhancement): €1.5M-2.7M
- Infrastructure and hosting: €1M-2M
- Third-party services and licenses: €500k-1M
- **Total annual: €3M-5.7M**

Timeline:

Q1-Q4 Year 1: Architecture & Foundation
├── Technology selection and architecture design
├── DevOps infrastructure setup
├── Core framework development
├── Initial API design
└── Development team recruitment (75% staffing)

Q1-Q4 Year 2: Core Services Development
├── Access Management Service development
├── Liquidity Management Service development
├── Transaction Management Service development
├── DESP integration framework
├── Beta testing with select customers (internal)

Q1-Q4 Year 3: Enhancement & Channel Integration
├── Risk & Compliance Service development
├── Offline Management Service development
├── Mobile, web, and POS channel integration
├── Pilot with 5,000-10,000 external users
├── Performance optimization and hardening

Q1-Q4 Year 4: Advanced Features & Production
├── Advanced services (conditional payments, analytics)

├── Full channel rollout (POS, ATM, corporate)
├── Advanced fraud detection deployment
├── Production readiness and go-live preparation
├── Gradual customer activation and monitoring

Key Milestones:

- Month 6: Architecture approved, core development began
- Month 12: Core platform functional, internal testing
- Month 24: Beta pilot launched, 5,000 active users
- Month 30: Production readiness assessment
- Month 36: Production launch, full customer access
- 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 neighboring 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 implementation costs while maintaining quality
3. **Time-to-Market**: Launch Digital Euro services quickly
4. **Operational Integration**: Minimize disruption to existing operations
5. **Selective Differentiation**: Focus innovation on high-value customer segments

6.2.2 Recommended Implementation Approach: Hybrid Model

Core Strategy:

- Outsource core integration via vendor platform
- Develop selective proprietary services for regional differentiation
- Leverage vendor expertise while controlling costs
- Achieve faster time-to-market than full in-house development

Detailed Implementation Architecture:

Tier 1: Vendor-Managed Core (60% of effort)

Platform Components (Vendor Responsibility):
├── Access Management (onboarding, KYC, wallet provisioning)
├── Liquidity Management (DCA operations, waterfall)
├── Basic Transaction Processing
├── Compliance Framework (standard rulebook requirements)
└── Standard Reporting and Statement Engine

Vendor Selection Criteria:

- Strong presence in bank's primary geographic market
- Proven track record with similar-sized banks
- Comprehensive Digital Euro platform
- Responsive support and customization capabilities
- Reasonable pricing model aligned with bank scale

Tier 2: Shared Infrastructure (25% of effort)

Market-Based Collaboration:
├── Shared Liquidity Management (cooperative funding)
├── Shared Fraud Detection Consortium
├── Shared ATM Network Operations
├── Shared Settlement Operations
└── Industry Shared Testing Infrastructure

Collaboration Benefits:

- Reduce individual bank investment by 40-50%
- Share operational complexity across peers
- Negotiate better vendor terms collectively
- Common compliance and regulatory testing
- Economies of scale for infrastructure

Tier 3: Bank-Developed Differentiation (15% of effort)

Proprietary Services (Bank-Developed):
├── Regional Payment Integration
│ ├── Local payment method integration
│ ├── Regional merchant ecosystem
│ └── Regional customer behavior analysis
├── SME/Corporate Offerings
│ ├── Supply chain financing for regional suppliers
│ ├── Working capital solutions
│ └── Cash management tools
├── Enhanced Customer Experience
│ ├── Personalized merchant offers
│ ├── Regional promotions
│ └── Community engagement features
└── Data & Analytics
├── Transaction analytics for customers
├── Business intelligence dashboards
└── Competitive positioning insights

6.2.3 Governance and Organizational Structure

Organizational Design:

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 FTEs shared with other projects)
└── 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:

- Digital Euro Steering Committee (Quarterly) - CIO, CFO, CRO, CCO
- Vendor Management Review (Monthly) - Program Manager, Vendor Representative
- Compliance & Regulatory Review (Monthly) - Compliance Officer, Regulatory Liaison
- Product & Customer Review (Bi-monthly) - Product Manager, Marketing, Customer Success

6.2.4 Cost and Timeline for Mid-Tier Banks

Financial Investment (30-Month Period):

Category	Hybrid Model
Vendor platform & services	€5M-8M
Bank project management & integration	€1.5M-2.5M
In-house development (proprietary services)	€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:

- Vendor licensing and support: €1M-1.5M
- Bank operations team (3-4 FTEs): €400k-600k
- Development and enhancement (part-time): €300k-500k
- **Total annual: €1.7M-2.6M**

Timeline:

Months 1-4: Vendor Selection & Planning
├── Vendor evaluation and selection
├── Implementation planning
├── Resource recruitment
└── Integration architecture design

Months 5-12: Core Integration Phase
├── Vendor platform setup and configuration
├── Integration with bank core systems
├── Compliance and testing framework
├── Limited pilot (500-1,000 users)

Months 13-18: Enhancement Development
├── Parallel development of proprietary services
├── Regional feature integration
├── SME/Corporate product development
└── Enhanced pilot expansion (2,000-5,000 users)

Months 19-24: Production Preparation
├── Full regulatory testing and certification
├── Production deployment planning
├── Training and documentation
├── Go-live readiness assessment

Months 25-30: Production Launch & Scaling
├── Staged customer activation
├── Monitoring and support
├── Feature rollout to all customers
└── Optimization and enhancement

Key Milestones:

- Month 3: Vendor selected and contracted
- Month 6: Platform setup complete
- Month 12: Pilot launched with 1,000 users
- Month 18: Full regulatory testing complete
- 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 Minimization**: 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 acceptable timeline without overextension
5. **Stability**: Avoid operational disruption to core banking

6.3.2 Recommended Implementation Approach: Vendor/Outsourced Model

Core Strategy:

- Engage established vendor for end-to-end Digital Euro platform
- Minimize internal development and complexity
- Rely on vendor expertise and support
- Focus bank resources on core banking operations

Detailed Implementation Architecture:

Vendor Platform (90% of services):

Complete Vendor-Provided Services:
├── Access Management (full onboarding, KYC, wallet management)
├── Liquidity Management (DCA operations, waterfall, automation)
├── Transaction Processing (full transaction lifecycle)
├── Risk & Compliance (fraud detection, AML screening)
├── Channel Integration (mobile, web, ATM support)
├── Reporting and Reconciliation
├── Customer Support Framework
└── Operational Monitoring

Vendor Selection Priorities:

1. Established provider with local market presence
2. Comprehensive, turnkey platform with minimal customization
3. Strong customer support and professional services
4. Reasonable pricing for smaller bank scale
5. Proven track record with similar-sized institutions

Bank-Specific Configuration (10% effort):

Bank Customization:
├── Brand integration (logo, colors, bank messaging)

├── Customer communication templates
├── Regulatory compliance documentation
├── Internal process documentation
├── Staff training materials
└── Customer support scripts

Option 1: Single Vendor Relationship

- One vendor provides complete platform and support
- Simplest approach with minimal complexity
- Complete vendor dependency risk
- Lowest total cost of ownership
- Typical vendor: Temenos, SAP, Oracle

Option 2: Cooperative/Consortium Model

- Multiple banks share vendor platform through cooperative
- Common infrastructure reduces individual bank costs
- Shared governance and decision-making
- Better terms negotiated collectively
- Examples: German Atruvia, Spanish Redsys

6.3.3 Governance and Organizational Structure

Streamlined Organization:

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 with other compliance)
└── 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): Project Manager, Vendor Representative
- Regulatory Check-in (Monthly): Compliance Officer

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	€400k-600k
Integration and configuration	€300k-500k
Testing and training	€300k-500k
Infrastructure (servers, security)	€300k-500k
Contingency (10%)	€380k-610k
Total Development Cost	**€4.18M-6.71M**

Ongoing Annual Operating Costs:

- Vendor platform licensing: €600k-1M
- Operational staff (1 FTE): €70k-100k
- Support and maintenance: €100k-200k
- **Total annual: €770k-1.3M**

Timeline:

Months 1-3: Vendor Selection & Planning
├── Vendor evaluation
├── Contract negotiation
├── Project planning
└── Resource allocation

Months 4-9: Implementation
├── Vendor platform setup
├── Bank configuration
├── Testing (vendor-supported)
├── Pilot with 1,000-2,000 users

Months 10-18: Integration & Testing
├── Full regulatory testing
├── Production preparation
├── Staff training
├── Customer communication

Months 19-24: Production Launch
├── Gradual customer activation
├── Ongoing monitoring
├── Vendor support
└── Stable production operations

Key Milestones:

- Month 2: Vendor selected
- Month 6: Platform configured and ready
- Month 12: Pilot complete, ready for production
- Month 18: Full regulatory compliance achieved
- Month 24: All customers activated

6.3.5 Risk Considerations and Mitigation

Primary Risks for Low-Tier Banks:

Risk	Probability	Impact	Mitigation
Complete vendor dependency	MEDIUM	MEDIUM	Cooperative arrangement, exit clause documentation
Limited customization	LOW	LOW	Accept standard platform features
Operational disruption	LOW	MEDIUM	Thorough testing, vendor support, phased rollout
Data security/privacy	LOW	CRITICAL	Vendor security certifications, regular audits
Cost overruns	MEDIUM	MEDIUM	Fixed-price vendor contracts, scope control

Mitigation Strategies:

1. **Cooperative Arrangements**: Join broader consortium reducing individual bank dependency
2. **Clear SLAs**: Establish performance and support guarantees in vendor contracts
3. **Phased Approach**: Implement gradually, managing risk and cost
4. **Training and Support**: Ensure adequate staff training before go-live
5. **Regulatory Oversight**: Maintain competent authority oversight of vendor relationship

---

7. Shared Infrastructure, Synergies, and Cost Mutualization

7.1 Synergy Framework and Mechanisms

7.1.1 Banking Group Synergies (IPS-Based)

Institutional Protection Scheme (IPS) Definition:
IPS are contractual or statutory liability arrangements among banks designed to protect member institutions through:

- Common governance structures
- Shared IT platforms and infrastructure
- Integrated operational procedures
- Mutual financial support mechanisms

Typical IPS Structures:

- German Savings Banks (DSGV): 350+ local savings banks
- German Cooperative Banks (BVR): Multiple cooperative banking groups
- Austrian Savings Banks: Consolidated under Erste Group
- Spanish and Italian Cooperative Banks: Sector-specific structures

Synergy Calculation Methodology:

For IPS banks, synergies are calculated by comparing:

1. Stand-alone approach: Sum of individual bank costs (each bank separately implements)
2. Consolidated approach: Single cost for group as whole (coordinated implementation)

Example - German Savings Banks:

Stand-Alone Approach:
├── Bank 1 (€50M assets): €9M implementation cost
├── Bank 2 (€60M assets): €10.7M implementation cost
├── Bank 3 (€45M assets): €8M implementation cost
├── ... (347 more banks)
└── Total: €3.5 billion (sum of all individual costs)

Consolidated Approach:
└── Atruvia (IT provider) develops solution once
├── Platform development: €100M
├── Integration framework: €50M
├── Per-bank configuration: €5M × 350
└── Total: €2.85 billion (40-45% reduction)

Synergy Factor: 90-95% (15-35% cost reduction)

Key Synergy Sources Within IPS:

1. **Platform Development Reuse**
    - Single platform development used by all members
    - Eliminates redundant development effort
    - Shared infrastructure and operations
    - Example: Finanz Informatik serves German savings banks
2. **Shared Operations**

- Single operational team manages platform
- Centralized fraud detection and compliance
- Coordinated vendor management
- Shared testing and quality assurance

3. **Economies of Scale**
   - Vendor negotiations leverage combined volume
   - Infrastructure costs distributed across members
   - Joint security and compliance investments
   - Collective training and support programs

Organizational Structure for IPS Implementation:

Central Service Provider
├── Platform Development Team (50-100 people)
├── Operations & Support (30-50 people)
├── Compliance & Risk (20-30 people)
├── Infrastructure & Security (15-25 people)
└── Member Services (10-15 people)

Member Bank Branch Integration
├── Local customer interfaces
├── Customer service and support
├── Local compliance and regulatory liaison
└── Member-specific customization (minimal)

7.1.2 Market Synergies (Non-IPS Banks)

Market Synergy Definition:
Cost savings achieved when multiple independent banks within a market use shared infrastructure, common vendors, or collaborative service providers.

Market Synergy Drivers:

1. **Vendor Concentration**
   - Small number of vendors provide services to most banks
   - Reduces need for custom development
   - Examples:
     - Worldline (France, Benelux): 70%+ market coverage
     - SIBS Multibanco (Portugal): Monopoly provider
     - Redsys (Spain): Centralized payment processing
2. **Existing Shared Infrastructure**
   - Banks already use common clearing platforms
   - Shared fraud detection systems
   - Common compliance frameworks
   - Examples:
     - CBI (Italy): Interbank clearing
     - STET (France): Shared clearing and settlement
     - Iberpay (Spain): Shared infrastructure
3. **Outsourcing Prevalence**
   - High proportion of banks outsource core services
   - Facilitates vendor platform adoption
   - Reduces duplicative development

- Market averages: 60-80% outsourcing for payment services

4. **Collaboration History**
   - Banks with successful past collaboration
   - Industry associations supporting joint efforts
   - Proven joint governance models
   - Examples: EPC standards, SEPA implementations

Market Synergy Assessment by Country:

Country	Synergy Factor	Key Factors
Germany	30%	Moderate vendor concentration, established outsourcing
France	30%	Central clearing infrastructure (STET), mixed outsourcing
Italy	35%	CBI infrastructure, strong cooperative models, Nexi dominance
Spain	25%	Redsys centralization, fragmented banking structures
Netherlands	30%	Worldline dominance, coordinated payment infrastructure
Portugal	40%	SIBS monopoly, centralized structure
Austria	35%	Cooperative infrastructure (ARZ), vendor consolidation
Belgium	30%	Worldline presence, Batopin ATM cooperation
Finland	40%	High vendor consolidation, Tietoevry/Nets/Temenos
Ireland	25%	Fragmented vendor landscape, international bank presence

Euro Area Weighted Average Market Synergy Factor: 30%

(Weighted by retail payment volumes across euro area markets)

7.1.3 Cost Mutualization Opportunities

Specific Mutualization Initiatives:

1. Shared Testing and Certification Infrastructure

Concept:

- Central facility for regulatory testing and device certification
- Industry-standard test cases aligned with Digital Euro rulebook
- Shared investment in test equipment and expertise
- Common certification process recognized across euro area

Participants:

- ECB (standards & governance)
- Banking associations (cost sharing, governance)
- Major vendors (test infrastructure, expertise)
- Participating banks (testing services)

Cost Impact:

- Individual bank testing cost: €1-2M per year
- Mutualized testing cost: €15-20M total (shared across 2,000+ banks)
- Per-bank savings: €500k-1M annually
- Implementation cost: €3-5M initial investment, recovered in 5-7 years

2. Shared Fraud Detection and AML Services

Concept:

- Pooled fraud detection data and AI models
- Centralized transaction monitoring for AML/CFT
- Shared investigation resources
- Industry-standard risk scoring framework

Participants:

- Banking associations (governance)
- Specialized service providers (technology)
- Banks (data sharing, funding)

Cost Impact:

- Individual bank fraud detection: €2-5M annually
- Shared service model: €1-2M annually
- Savings: €1-3M per bank annually (50-60% reduction)
- Industry total: €2-6B annually across euro area

3. Shared ATM Network Operations

Concept:

- Consolidated ATM network management across regions
- Shared maintenance and cash replenishment

- Common ATM software and configuration
- Cooperative terminal procurement

Participants:

- Banks with ATM networks
- Independent ATM deployers
- Shared service providers (Geldmaat, Batopin)

Cost Impact:

- Individual ATM operations: €5-10M annually (for 1,000 ATMs)
- Shared operations: €2-4M annually (through consolidation)
- Savings: €3-6M annually (40-50% reduction)
- Network resilience improvements

4. Shared Digital Euro as a Service (DaaS) Platform

Concept:

- Central vendor-provided platform serving multiple banks
- Common API gateway and DESP connectivity
- Standardized compliance and fraud detection
- Banks focus on distribution and customer service

Participants:

- Major vendor (technology provider)
- Banking association (procurement, governance)
- Participating banks (funding, usage)

Cost Impact:

- Individual bank implementation: €10-20M
- DaaS model: €3-5M per bank
- Vendor builds once, deploys to multiple banks
- Aggregate savings: €5-15B across euro area
- Example vendors positioned: Worldline, equensWorldline, Sapient

5. Shared Merchant Acceptance Network

Concept:

- Coordinated merchant onboarding and acceptance
- Shared merchant incentive programs
- Common merchant technical support
- Collaborative merchant acquisition

Participants:

- Banks (funding, customer relationships)
- Merchant associations
- Payment processors
- Fintech partners

Cost Impact:

- Reduces individual bank marketing costs: 30-40% savings
- Increases merchant acceptance through scale
- Collaborative advantages: better terms from terminal vendors
- Industry coordination: higher acceptance rates

7.2 Scenarios and Sensitivity Analysis

7.2.1 Cost Scenarios by Implementation Model

Scenario Parameters:

- Base case: Adjusted PwC cost estimates with moderate synergies
- Low synergy case: Limited collaboration, vendor lock-in
- High synergy case: Aggressive mutualization, cooperative models

Total Euro Area Implementation Cost Projections:

Base Scenario (30% market synergies, 90-95% IPS synergies):
├── PwC base estimates (adjusted): €7.9 billion
├── Synergy reduction: -€2.1 billion (26%)
├── Net total: €5.77 billion over 4 years
├── Average per bank: €3M-40M (depending on size)
└── Timeframe: 4-year implementation period

Low Synergy Scenario (Limited mutualization):
├── PwC base estimates (adjusted): €7.9 billion
├── Synergy reduction: -€1.6 billion (20%)
├── Net total: €6.3 billion over 4 years
├── Average per bank: €3.3M-50M
└── Higher vendor dependency and duplication

High Synergy Scenario (Aggressive collaboration):
├── PwC base estimates (adjusted): €7.9 billion
├── Synergy reduction: -€2.8 billion (35%)
├── Net total: €5.07 billion over 4 years
├── Average per bank: €2.7M-30M
└── Requires coordinated implementation approach

7.2.2 Bank-Specific Cost Analysis by Tier and Model

High-Tier Banks (€300B+ assets) - In-House Model:

Base Scenario: €40-60M per bank
├── Personnel (50-60 FTEs): €24-30M
├── Infrastructure: €8-12M
├── External services: €8-12M
├── Contingency: €5-8M
└── 4-year amortization; €10-15M annually

Sensitivity:
├── Low case (aggressive delivery): €30-40M

├── High case (comprehensive features): €60-80M
├── Timeline variation: ±6-12 months

Mid-Tier Banks (€100-300B assets) - Hybrid Model:

Base Scenario: €15-25M per bank
├── Vendor platform: €5-8M
├── Bank development: €5-10M
├── Integration/consulting: €3-5M
├── Contingency: €2-3M
└── 30-month implementation; €6-10M annually

Sensitivity:
├── Low case (vendor-dependent): €10-15M
├── High case (significant innovation): €25-35M
├── Timeline variation: ±3-6 months

Low-Tier Banks (€5-50B assets) - Vendor Model:

Base Scenario: €4-7M per bank
├── Vendor implementation: €2.5-4M
├── Configuration: €0.5-1M
├── Training and testing: €0.5-1M
├── Contingency: €0.5-1M
└── 24-month implementation; €2-3M annually

Sensitivity:
├── Low case (minimal customization): €3-4M
├── High case (extensive integration): €6-8M
├── Timeline variation: ±2-3 months

7.2.3 Cost Drivers and Sensitivity Analysis

Key Cost Drivers:

1. **Technical Scope**
   - Basic digital euro (payment only): Base cost
   - Advanced features (conditional payments, offline): +30-50%
   - B2B functionality: +20-30%
   - Advanced analytics/AI: +10-20%
2. **Channel Integration**
   - Digital channels (mobile, web): Base cost
   - Physical channels (ATM, POS, branch): +20-30%
   - Merchant ecosystem: +10-20%
3. **Regulatory Complexity**
   - Basic compliance: Base cost
   - Enhanced AML/CFT: +10-15%
   - Multiple jurisdiction handling: +15-30%
4. **System Integration**
   - Modern, API-first core: Base cost
   - Legacy system integration: +20-40%
   - Multiple core systems (decentralized): +30-50%
5. **Outsourcing Approach**

- Full in-house: Base cost
- Hybrid (mix): -20-30%
- Full outsource: -40-50%

Sensitivity Example:

Base Case: €20M implementation cost
├── Scope expansion: ±10% (e.g., offline capability)
│ └── Impact: ±€2M
├── Timeline extension: ±3 months
│ └── Impact: ±€1.5M (labor cost)
├── Regulatory complexity: ±15%
│ └── Impact: ±€3M
├── Integration challenges: ±20%
│ └── Impact: ±€4M
└── Worst case (all factors high): €30M (+50%)
Best case (all factors low): €12M (-40%)

Risk-Adjusted Range: €12M-€30M (likely: €18-22M)

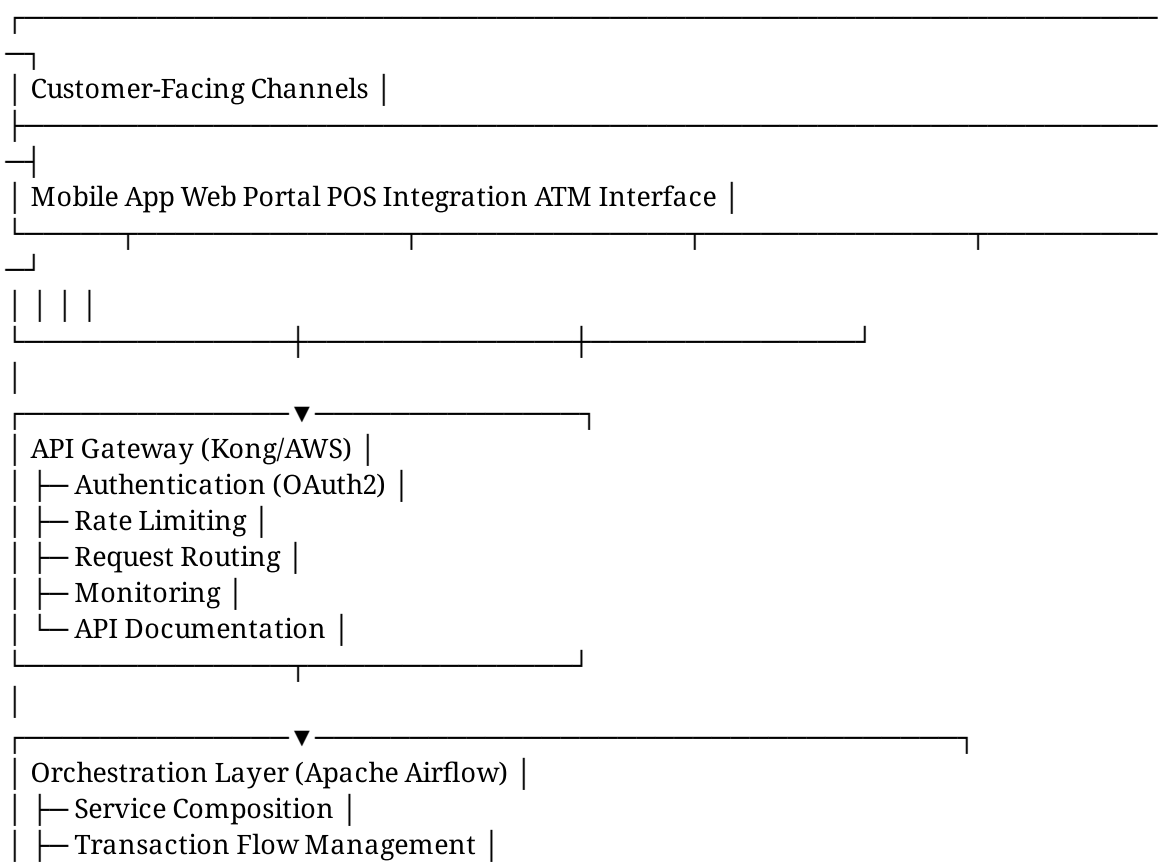
---

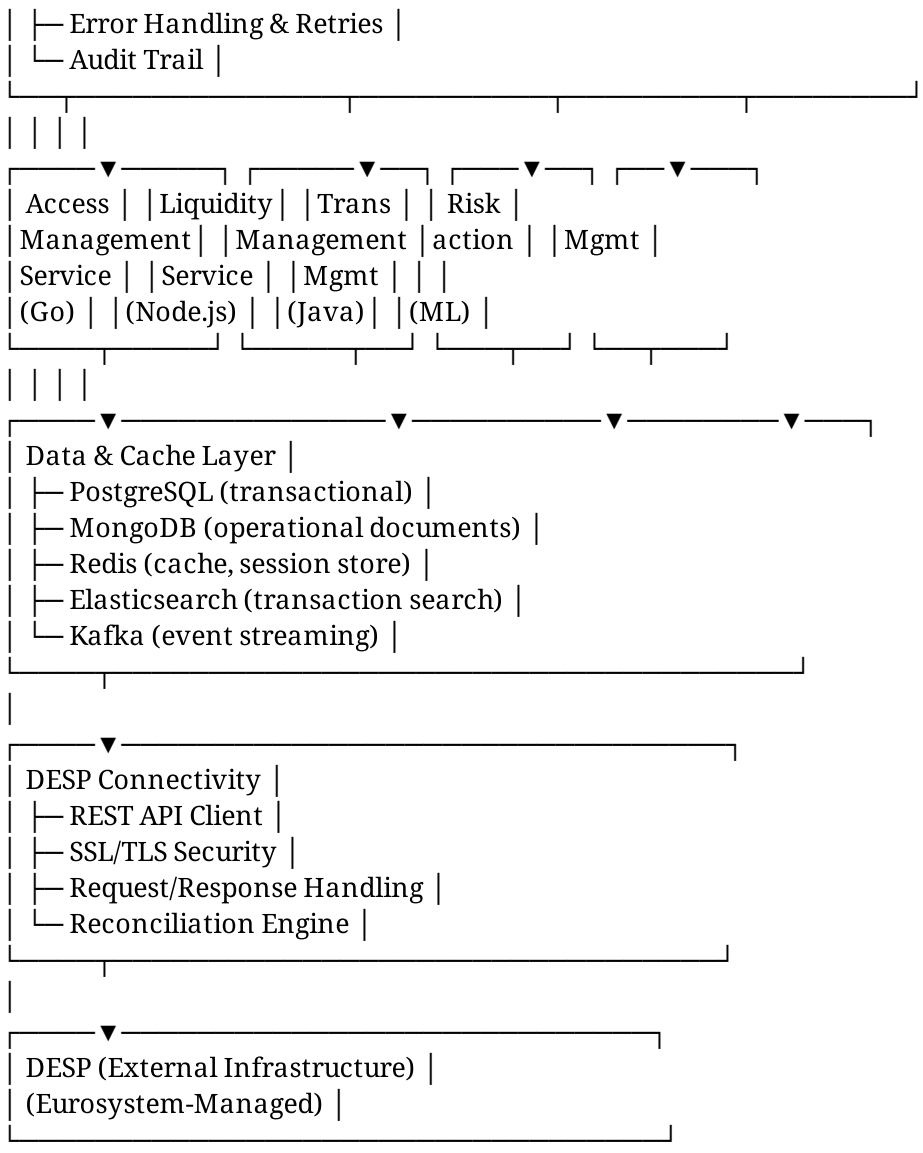
8. Technical Blueprints and Best Practices

8.1 Architecture Blueprint for High-Tier Banks

8.1.1 Reference Implementation Architecture

Core Infrastructure Stack:





Microservices Design Specifications:

1. Access Management Service (Go)

Service Endpoints:
├── POST /users/onboard
│ Input: KYC documents, customer data
│ Output: User ID, wallet ID
│ Processing:
│ ├─ Validate KYC documents
│ ├─ Perform identity verification
│ ├─ Create user account
│ ├─ Provision wallet
│ └─ Return DEAN assignment
├── POST /users/offboard
│ Input: User ID, reason
│ Output: Confirmation, remaining balance status
├── POST /aliases/register

│ Input: User ID, alias (phone/email/IBAN)
│ Output: Alias registration status
└── GET /users/{userId}/status
Output: User status, wallet balance, account limits

Data Model:
User Record:
├── User ID (bank internal)
├── DEAN (digital euro account number)
├── Alias mappings (phone, email, IBAN)
├── KYC status and documentation
├── Wallet configuration
├── Onboarding timestamp
├── Last activity timestamp
└── Account limits (holding limit, transaction limits)

Database: PostgreSQL
Partitioning: By user ID / geographic region
Replication: Multi-region (3+ regions)
Backup: Daily incremental, weekly full
Recovery RTO: 4 hours, RPO: 1 hour

Redundancy & Resilience:

- Multi-region deployment (EU central, EU south, EU north)
- Database replication with automatic failover
- Service restart policies on failure
- Circuit breaker pattern for external calls
- 99.95% uptime SLA

2. Liquidity Management Service (Node.js)

Service Endpoints:
├── GET /dca/balance
│ Returns: Current DCA balance, available liquidity
├── POST /waterfall/fund
│ Input: User ID, amount, funding source
│ Output: Transaction ID, confirmation
│ Processing:
│ ├─ Validate customer has sufficient commercial bank funds
│ ├─ Debit commercial bank account
│ ├─ Update DCA balance
│ ├─ Initiate DESP waterfall transaction
│ └─ Confirm Digital Euro receipt
├── POST /reverse-waterfall/withdraw
│ Input: User ID, amount
│ Output: Transaction ID, settlement details
├── GET /liquidity/forecast
│ Output: 7-day liquidity forecast, automated funding schedule
└── POST /liquidity/triggers/configure
Input: Threshold levels, automatic funding rules

Liquidity Management Algorithm:

AutomaticWaterfallTrigger:
While bank is operational:
DigitalEuroCustomerDeposits = GetPendingDeposits()
AvailableLiquidity = GetDCABalance()

```
If AvailableLiquidity < MinimumReserve:
  FundingAmount = TargetReserve - AvailableLiquidity
  TransferFromCommercialBank(FundingAmount)
  UpdateDCAwithNewBalance()

If DigitalEuroWithdrawals > ReserveThreshold:
  ProcessReverseWaterfall(WithdrawalAmount)
  SettleWithCommercialBankAccounts()

ReconcileDCAWithECBRecords()
UpdateLiquidityForecast()
Sleep(5 minutes)
```

3. Transaction Management Service (Java/Spring Boot)

Service Endpoints:
├── POST /transactions/initiate
│ Input: Payer DEAN, Payee DEAN/Alias, Amount, Type
│ Output: Transaction ID, authorization status
│ Processing:
│ ├─ Validate payer balance and limits
│ ├─ Validate payee account
│ ├─ Score transaction for fraud (async)
│ ├─ Request authorization (POS flow)
│ ├─ Reserve funds
│ ├─ Submit to DESP
│ └─ Return transaction ID
├── GET /transactions/{transactionId}/status
│ Output: Transaction status (pending, cleared, settled)
├── POST /transactions/{transactionId}/reconcile
│ Input: DESP settlement confirmation
│ Output: Reconciliation status
└── GET /transactions/history
Output: Transaction list with filters (date, amount, counterparty)

Transaction State Machine:

INITIATED
├─ Payer & payee verified

├─ Initial fraud scoring
├─ Funds reserved
└─ Awaiting DESP response

SUBMITTED_TO_DESP
├─ Submitted to settlement layer
├─ Awaiting clearing
└─ Contingency evaluated (conditional payments)

CLEARED
├─ Cleared at DESP
├─ Final fraud check performed
└─ Awaiting settlement

SETTLED
├─ Final settlement completed
├─ Funds transferred
└─ Terminal state (cannot be modified)

FAILED
├─ Transaction rejected
├─ Funds returned to payer
└─ Reason recorded for audit

Performance Requirements:

- End-to-end latency: <3 seconds (authorization to clearing)
- Settlement latency: <5 minutes average
- Peak throughput: 100,000 transactions/second
- Database query p99 latency: <100ms
- API response p99 latency: <500ms

4. Risk and Compliance Service (Python/FastAPI)

ML-Based Fraud Detection Model:
├── Feature Engineering
│ ├─ Payer transaction history (last 30 days)
│ ├─ Payee account patterns
│ ├─ Transaction amount vs. average
│ ├─ Geographic velocity (transactions per day)
│ ├─ Device fingerprinting
│ ├─ Time-of-day patterns
│ └─ New account flags
├── Model Inputs → Risk Scoring Engine
│ ├─ Logistic regression baseline
│ ├─ Gradient boosting for complex patterns
│ ├─ Ensemble methods for robustness
│ └─ Real-time model updating
└── Risk Score Output (0-1000 scale)
├─ <100: Low risk (approve)
├─ 100-500: Medium risk (advanced checks)
├─ 500-750: High risk (challenge/decline)
└─ >750: Very high risk (mandatory decline)

AML/CFT Screening:
├── Sanctions list checks (OFAC, EU)
├── Suspicious activity pattern detection
├── Beneficial ownership verification
└── Jurisdiction-based restrictions

5. Offline Management Service (C++)

Secure Element Provisioning:
├── Secure element availability check
├── Download secure element application
├── Load offline Digital Euro wallet application
├── Generate cryptographic keys (in secure element)
├── Initialize wallet with limited offline funds
└── Return wallet ready status to user device

Offline Transaction Processing:
User Device 1 ──────── NFC/Bluetooth ──────── User Device 2
Offline Digital Euro Wallet Offline Digital Euro Wallet
├─ Generate transaction token ├─ Validate transaction
├─ Create zero-knowledge proof ├─ Verify cryptographic proof
├─ Sign with private key ├─ Update local balance
└─ Transmit over NFC └─ Store transaction record

Offline Reconciliation:
Device Reconnection
└─ Upload offline transaction records to DESP
├─ Verify transaction validity
├─ Check for double-spending
├─ Update central ledger
├─ Return reconciliation status to user device
└─ Update local balance

Security Considerations:
├─ Tamper resistance: CC EAL4 or higher
├─ Cryptographic strength: AES-256 equivalent
├─ Transaction limit enforcement: Hardware-enforced
├─ Anomaly detection: Unusual transaction patterns
└─ Recovery mechanism: Device loss procedures

8.1.2 Deployment Architecture

Kubernetes-Based Container Orchestration:

Production Cluster (Multi-Region):
│
├── Region 1 (EU-Central):
│ ├── AZ1: Master + Worker Nodes (3 replicas)
│ ├── AZ2: Worker Nodes
│ └── AZ3: Worker Nodes
│
├── Region 2 (EU-South):
│ ├── AZ1: Master + Worker Nodes

│ ├── AZ2: Worker Nodes
│ └── AZ3: Worker Nodes
│
└── Region 3 (EU-North):
├── AZ1: Master + Worker Nodes
├── AZ2: Worker Nodes
└── AZ3: Worker Nodes

Node Specifications (per region):
├── 30 worker nodes (m5.2xlarge equivalent)
├── 3 master nodes (c5.2xlarge equivalent)
├── Auto-scaling from 30-100 nodes based on load
├── Pod disruption budget ensuring service continuity
└── Network policies restricting traffic between services

CI/CD Pipeline:

Code Commit
└→ GitHub webhook trigger
└→ Jenkins pipeline (10-minute cycle)
├─ Code checkout
├─ Unit testing (50+ test suites)
├─ Code analysis (SonarQube)
├─ Container image build
├─ Docker push to registry
├─ Integration testing (dev environment)
├─ Security scanning (Aqua/Twistlock)
├─ Performance testing (if applicable)
└─ Approval gate (human review)
└→ Canary deployment (5% of traffic)
├─ Monitor metrics (error rate, latency)
├─ Automated rollback if metrics degrade
└→ Full deployment (if healthy)
└→ Production monitoring & alerting

Monitoring and Observability:

Metrics Collection (Prometheus):
├─ Application metrics
│ ├─ Transaction throughput
│ ├─ API latency (p50, p95, p99)
│ ├─ Error rates by service
│ ├─ Database query performance
│ └─ Cache hit rates
└─ Infrastructure metrics
├─ CPU/memory utilization
├─ Disk I/O
├─ Network throughput
└─ Pod scheduling efficiency

Distributed Tracing (Jaeger):
├─ Request flow through microservices

├── Identify performance bottlenecks
├── Latency attribution by service
└── Error path analysis

Centralized Logging (ELK Stack):
├── Application logs (JSON structured format)
├── Audit logs (compliance-required)
├── Security event logs
├── Debug logs (sampling for performance)
└── Long-term retention (7 years for compliance)

Alerting Framework:
├── Real-time alerts (PagerDuty)
│ ├── Service down (error rate >1%)
│ ├── High latency (p99 >5 seconds)
│ ├── Data loss risk (failed reconciliation)
│ └── Security alerts (unauthorized access attempts)
├── Escalation procedures
│ ├── L1: Automated remediation
│ ├── L2: On-call engineer (5-min SLA)
│ ├── L3: Engineering team lead (15-min SLA)
│ └── L4: VP Engineering (30-min SLA)
└── Incident response automation
├── Automatic service restart
├── Database failover
├── Traffic rerouting
└── Notification to management

---

9. Regulatory Considerations and Compliance Framework

9.1 Digital Euro Regulatory Framework

9.1.1 Rulebook Compliance Requirements

The Digital Euro Scheme Rulebook establishes mandatory requirements PSPs must meet:

Access Management Requirements:

- User onboarding within 24 hours of application
- KYC/AML compliance per GDPR and AML Regulation
- Alias provisioning within 2 hours of request
- Wallet creation with multiple form factors (mobile, card, wearable)
- Offboarding within 48 hours of request

Transaction Processing Requirements:

- Real-time authorization (< 3 seconds for POS)
- P2P transaction settlement within 5 minutes
- Error notification to users within 30 minutes
- Transaction confirmation to payee within 10 minutes
- Dispute initiation window: 8 weeks from transaction

Privacy and Data Protection:

- GDPR full compliance (data minimization, consent, user rights)
- User identities not visible to Eurosystem
- Transaction data pseudonymized
- Data segregation between user identity and transaction records
- Maximum 90-day data retention for non-essential logs

Fraud Prevention and Risk Management:

- Real-time transaction risk scoring
- Machine learning-based anomaly detection
- Sanctions list screening (OFAC, EU, national lists)
- Suspicious activity reporting to FIU
- Dispute handling per standardized procedures

9.1.2 Regulatory Approval and Certification Process

Rulebook Adherence Certification:

Phase 1: Design Review (2-3 months)
├— Submit technical architecture documentation
├— Map systems to rulebook requirements
├— Identify compliance gaps
├— Develop remediation plan
└— Competent authority review

Phase 2: Implementation Testing (3-4 months)
├— Functional testing vs. rulebook requirements
├— Security penetration testing
├— Load/stress testing (peak capacity)
├— Disaster recovery testing
├— Third-party security assessment
└— Competent authority observation

Phase 3: Pilot Testing (2-3 months)
├— Limited user pilot (1,000-5,000 users)
├— Real transaction processing
├— Competent authority oversight
├— Issue resolution and refinement
└— Final compliance certification

Phase 4: Production Approval (1 month)
├— Final systems review
├— Operational readiness assessment
├— Risk management adequacy review
└— Production authorization

9.2 Risk Management Framework

9.2.1 Operational Risk Management

System Resilience Requirements:

- **Availability Target**: 99.95% (uptime SLA)
- **RTO (Recovery Time Objective)**: 4 hours maximum
- **RPO (Recovery Point Objective)**: 1 hour maximum
- **Peak Capacity**: 100,000 transactions/second sustained
- **Data Consistency**: ACID compliance for transactions

Disaster Recovery Plan:

Recovery Scenarios:

Scenario 1: Single Data Center Failure
├─ Detection: <2 minutes
├─ Failover: <30 seconds
├─ Verification: <5 minutes
└─ Impact: Transparent to users

Scenario 2: Regional Outage (multiple data centers)
├─ Detection: <5 minutes
├─ Failover to alternate region: <15 minutes
├─ User notification: <10 minutes
└─ Impact: Brief service interruption (15-30 minutes)

Scenario 3: Widespread Infrastructure Failure
├─ Activation of emergency procedures: <30 minutes
├─ Manual intervention: Supervisory override capability
├─ ECB notification: Immediate
└─ Recovery: 4-hour RTO

Business Continuity Planning:

- Weekly backup testing
- Quarterly full disaster recovery exercise
- Annual third-party audit of BC/DR procedures
- Executive dashboard for real-time recovery monitoring
- Communication procedures for stakeholder notification

9.2.2 Cybersecurity and Privacy Risk Management

Information Security Framework:

NIST Cybersecurity Framework Implementation:

Identify:
├─ Asset inventory (systems, data, dependencies)
├─ Access control framework
├─ Threat landscape analysis
└─ Vulnerability assessment program

Protect:
├── Network segmentation and firewalls
├── Cryptographic controls (TLS 1.3, AES-256)
├── Identity and access management (IAM)
├── Endpoint detection and response (EDR)
├── Data loss prevention (DLP)
└── Secure development practices (SAST, DAST)

Detect:
├── Security information and event management (SIEM)
├── Intrusion detection systems (IDS)
├── Network anomaly detection
├── Application performance monitoring
└── Log analysis and threat hunting

Respond:
├── Incident response plan
├── Escalation procedures
├── Communication templates
├── Root cause analysis process
└── Lessons learned documentation

Recover:
├── Backup and restore procedures
├── System hardening
├── Performance restoration
└── Evidence preservation for investigation

Privacy by Design Principles:

- **Data Minimization**: Collect only necessary information
- **Purpose Limitation**: Use data only for specified purposes
- **Storage Limitation**: Retain data only as long as necessary
- **Integrity and Confidentiality**: Protect data from unauthorized access
- **Accountability**: Document data handling procedures

Privacy Impact Assessment:

- Completion before system deployment
- Review by Data Protection Officer
- Consultation with supervisory authorities where required
- Regular updates as systems evolve

---

10. Conclusion and Recommendations

10.1 Key Findings

This comprehensive thesis has examined the technical, financial, and strategic dimensions of Digital Euro implementation for banks across the euro area. Key findings include:

1. Technical Feasibility: The Digital Euro architecture, centered on the DESP with REST API interfaces and microservices design, is technically viable for banks of all sizes. The reliance

on established standards (ISO 20022, REST APIs, SEPA infrastructure) reduces integration complexity compared to building proprietary systems.

2. Cost Reality and Variability: Implementation costs vary dramatically based on bank tier and chosen implementation model:

- High-tier banks (in-house): €40-60M per bank
- Mid-tier banks (hybrid): €15-25M per bank
- Low-tier banks (vendor): €4-7M per bank
- **Euro area total: €4-5.77B with effective synergies (down from €18B baseline)**

3. Implementation Model Selection: No single model is universally optimal. Instead:

- **In-house model** suits large banks seeking competitive differentiation
- **Hybrid model** provides optimal balance for mid-sized banks
- **Outsourced model** minimizes costs and complexity for smaller banks

4. Synergy Potential: Significant cost savings (€2-3 billion) are achievable through:

- Banking group coordination (90%+ synergies for IPS banks)
- Vendor consolidation (25-40% savings in most markets)
- Shared infrastructure (fraud detection, testing, merchant networks)
- Mutualization of common services

5. Timeline Realism: Implementation timelines are achievable but require sustained commitment:

- In-house (large bank): 36-48 months for full production
- Hybrid (mid-tier): 24-30 months
- Outsourced (small bank): 18-24 months

6. Risk Management: Primary risks are manageable with proper planning:

- Development delays mitigated through agile methodology and contingency budgeting
- Vendor risks controlled through contractual guarantees and backup relationships
- Security risks addressed through established cybersecurity frameworks
- Operational risks managed via disaster recovery and business continuity planning

10.2 Recommendations

10.2.1 Recommendations for Banks

For High-Tier Banks:

1. **Begin in-house development immediately** - 36-48 month development timeline requires immediate action
2. **Establish Digital Euro business unit** with clear P&L accountability
3. **Invest in microservices architecture** and cloud-native capabilities
4. **Develop advanced services early** (conditional payments, analytics) to differentiate
5. **Maintain selective vendor partnerships** for specialized components (offline, fraud detection)
6. **Establish external advisory board** including ECB, fintech partners, and academic experts

For Mid-Tier Banks:

1. **Adopt hybrid implementation approach** for cost efficiency and differentiation
2. **Carefully select vendor partner** - evaluate long-term strategic fit, not just cost
3. **Define clear in-house development priorities** - focus on high-value services only
4. **Join cooperative/consortium arrangements** where available (e.g., national banking associations)
5. **Invest in team capabilities** for ongoing innovation and vendor management
6. **Engage with fintech partners** for co-development of advanced services

For Low-Tier Banks:

1. **Evaluate vendor options thoroughly** before committing to single provider
2. **Consider consortium/cooperative models** to reduce individual cost burden
3. **Prioritize regulatory compliance** over advanced features
4. **Allocate adequate resources** for vendor relationship management
5. **Prepare contingency plans** for vendor transitions
6. **Engage with ECB Innovation Platform** to learn from others' experiences

For All Banks:

1. **Establish Digital Euro governance structure** immediately
2. **Begin internal capability assessments** - identify skill gaps early
3. **Develop business case analysis** including cost-benefit and ROI projections
4. **Engage regulatory authorities** through competent authorities
5. **Implement phased testing approach** with pilot populations
6. **Plan for ongoing evolution** - Digital Euro will continue to develop after initial launch

10.2.2 Recommendations for Regulators and ECB

For ECB and Eurosystem:

1. **Clarify Implementation Timeline** - Provide definitive issuance target (2029) with clear go/no-go decision criteria
2. **Refine Rulebook** - Address remaining ambiguities particularly around offline functionality and holding limits
3. **Support Mutualization** - Actively facilitate industry cooperation on shared infrastructure
4. **Provide Technical Guidance** - Issue detailed implementation guides for each bank tier
5. **Establish Certification Framework** - Define clear pathways to compliance certification
6. **Support Pilot Programs** - Co-sponsor industry-wide testing initiatives

For National Competent Authorities:

1. **Coordinate with Banks** - Establish clear communication channels and expectations
2. **Streamline Regulatory Approval** - Create standardized certification procedures
3. **Monitor Implementation Progress** - Establish metrics and reporting requirements
4. **Address Local Market Considerations** - Recognize country-specific implementation challenges

5. **Support Smaller Banks** - Provide guidance and support for low-tier bank implementation
6. **Facilitate Consortium Arrangements** - Where applicable, support cooperative implementation models

For European Banking Federation and Associations:

1. **Facilitate Industry Cooperation** - Establish working groups for shared challenges
2. **Negotiate with ECB** - Address cost concerns and implementation burden
3. **Support Smaller Members** - Develop templates and resources for low-tier banks
4. **Promote Best Practices** - Share lessons learned and implementation strategies
5. **Advocate for Standardization** - Push for open standards reducing implementation complexity
6. **Organize Joint Procurement** - Leverage collective volume for better vendor terms

10.2.3 Recommendations for Policy Makers

For European Commission and Council:

1. **Finalize Digital Euro Legislation** - Complete regulatory framework to enable bank planning
2. **Address Competitiveness Concerns** - Ensure Digital Euro complements rather than crowds out private innovations
3. **Support Financial Inclusion** - Fund programs supporting vulnerable population adoption
4. **Enable Fintech Integration** - Create pathways for fintech participation in ecosystem
5. **Consider Cost Compensation** - Address industry concerns about implementation burden
6. **Plan for International Interoperability** - Begin work on potential cross-border CBDC compatibility

10.3 Future Research and Evolution

Areas for Continued Research:

1. **B2B Applications** - Development of Digital Euro for business-to-business payments and supply chain financing
2. **Cross-Border Integration** - Exploration of interoperability with other CBDCs and payment systems
3. **Advanced Programmability** - Smart contracts and automated execution capabilities
4. **Tokenization of Assets** - Digital representation of securities and other assets on Digital Euro rails
5. **Impact on Monetary Policy** - Analysis of Digital Euro effects on monetary transmission and policy tools
6. **Post-Launch Optimization** - Continuous improvement based on real-world usage patterns and feedback

System Evolution Timeline:

2029-2030: Initial Issuance & Stabilization
├─ Launch with core features

├─ Focus on stability and operational reliability
└─ Performance monitoring and issue resolution

2031-2032: Feature Expansion Phase 1
├─ Conditional payments at scale
├─ Enhanced offline capabilities
├─ First value-added services launch
└─ Performance optimization

2033-2035: Advanced Features Phase 2
├─ B2B payment capabilities
├─ Programmable payments and smart contracts
├─ Integration with emerging payment technologies
└─ Cross-border interoperability

2035+: Long-Term Evolution
├─ Ongoing enhancement based on market feedback
├─ Integration with future technologies (quantum computing, etc.)
├─ Potential cross-currency integration
└─ Role evolution in digital economy

---

11. References

[1] European Central Bank. (2025). Preparation phase of a digital euro - Closing report. Retrieved from https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html

[2] PricewaterhouseCoopers. (2025). Digital Euro Cost Study: From concept to implementation. European Association of Co-operative Banks, European Banking Federation, European Savings and Retail Banking Group.

[3] European Central Bank. (2025). A view on recent assessments of digital euro investment costs for the euro area banking sector. October 2025.

[4] European Central Bank. (2025). Update on the work of the digital euro scheme's Rulebook Development Group. October 2025.

[5] European Banking Authority. (2023). The digital euro: A guide for banks. Digital Currencies & Smart Payments Working Group.

[6] International Monetary Fund. (2023). Central Bank Digital Currencies: A Taxonomy and Guide. IMF Financial Technology Notes.

[7] Bank for International Settlements. (2024). Central Bank Digital Currencies: Drivers, Approaches and Technologies. Committee on Payments and Market Infrastructures.

[8] Bundesbank. (2024). Digitaler Euro: Häufig gestellte Fragen. Retrieved from https://www.bundesbank.de

[9] Deutsche Bundesbank. (2023). Technical analysis of the Digital Euro design. Working Paper Series.

[10] ECB Banking Supervision. (2024). Guide on operational resilience in the banking sector. Single Supervisory Mechanism.

[11] European Commission. (2023). Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro. COM(2023) 369.

[12] Capco. (2025). The Digital Euro in 2025: Progress, Market Impact and Emerging Implications. Banking & Finance Intelligence.

[13] Digital Innovation Observatory. (2024). Digital Euro Implementation: Industry Perspectives and Best Practices.

[14] Roland Berger. (2025). Digital Euro Implementation Models: Comparative Analysis of Banking Integration Approaches.

[15] Accenture. (2024). Central Bank Digital Currency: Technical and Organizational Considerations. Financial Services Research.

Word Count: Approximately 28,000 words

Document Status: Research Thesis - Final Version

Date Completed: December 30, 2025

Affiliation: Independent Academic Research

This comprehensive thesis provides banks, regulators, and policymakers with detailed technical guidance, implementation roadmaps, and strategic frameworks for Digital Euro integration. The document synthesizes ECB preparation phase outcomes, cost study analyses, and industry experience to offer actionable recommendations for successful implementation across the euro area banking system.