

Secure and Resilient PFM Systems

JULY 04, 2025

Alok Verma
Fiscal Affairs Department

Picture Credits: AAAG

Why secure and resilient PFM Systems?



Growing digitalization of budget execution, accounting, and reporting systems



Rising threats- cyberattacks, frauds, data breaches, ransomware in government systems



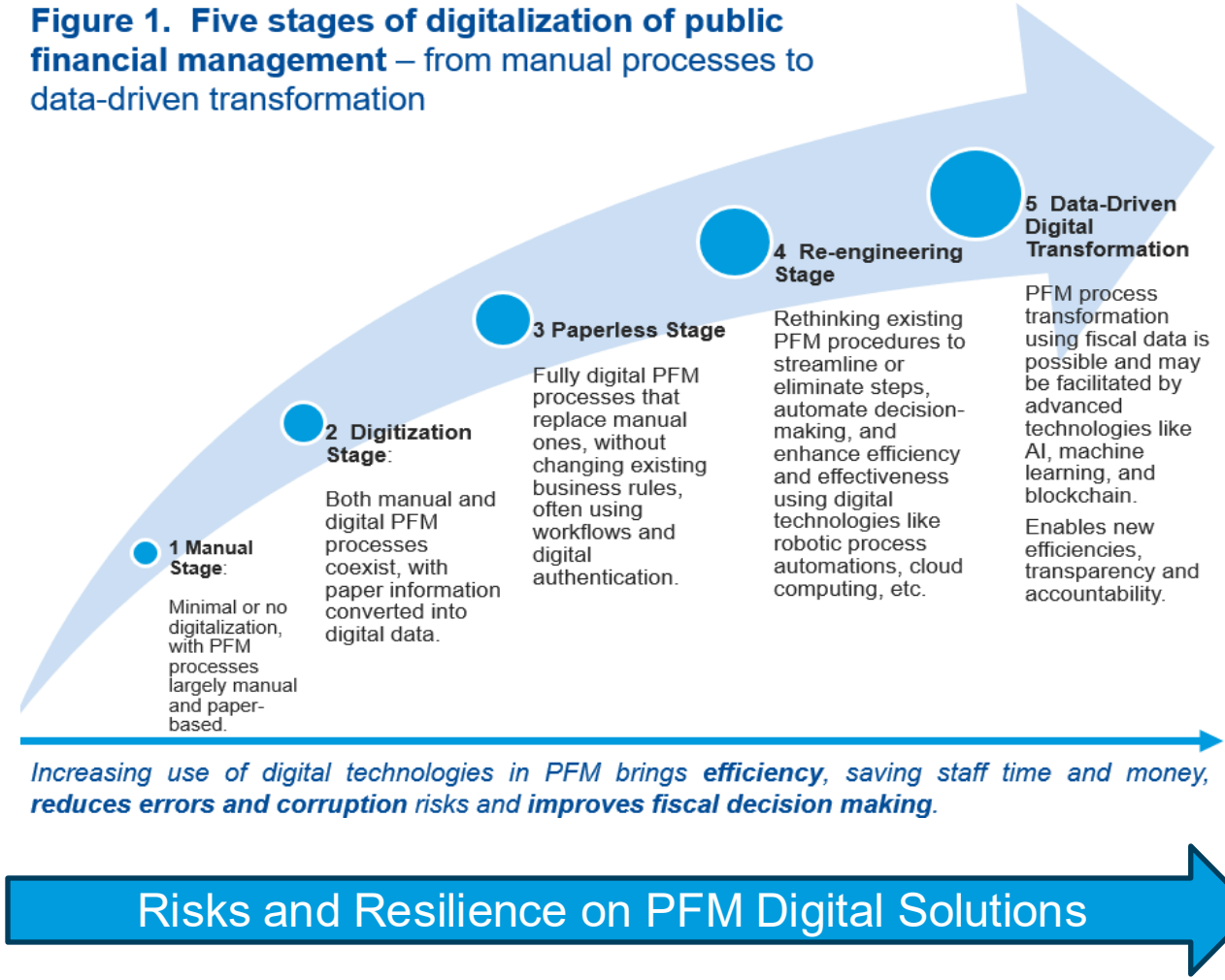
Integrity of fiscal data is essential for trust, transparency, and continuity



Resilient PFM Systems are foundational for service delivery in crises

Stages of Digitalization: Risk and Resilience

Figure 1. Five stages of digitalization of public financial management – from manual processes to data-driven transformation



Advanced stages of digitalization require enhanced risk management and resilience practices to safeguard critical PFM operations.

Digitalization Framework: Secure and Resilient PFM Digital Ecosystem

	Manual (1)	Digitization (2)	Paperless (3)	Re-Engineering (4)	Transformation (5)
External Environment	BPM-Manual	BPM-Digitization	BPM-Paperless	BPM- Re-engineering	BPM-Transformation
PFM IT Systems Features (F)	Not Applicable	+Data quality controls (F2.1) +Audit trails (F2.2) +Document management system (F2.3) + Business Process Integration (F2.4)	+Digital signature (F3.1) +Exception reports/alerts (F3.2) +Workflow configurations (F3.3) + Interoperability (F3.4) +Process specific internal controls (F3.5) +High Availability (F3.6)	+Interoperable Architecture (F4.1) +Microservices Architecture (F4.2) +Scalability (F4.3) +Agility (F4.4) +Suitable Data Architecture (4.5)	+Smart contracts (F5.1) +Advanced data analytics (F5.2) +Cognitive Automation (F 5.3)
Fiscal Data Governance (D)	+Availability reliable financial accounts data (D1.1)	+ Master and reference data (D2.1) +Reliable transaction data (D2.2)	+Data Registers (metadata) (D3.1) +Data Quality Control Framework (D3.2)	+Established FDG Program (D4.1) +Open Data to facilitate reuse and repurposing (D4.2)	+Big data (D 5.1) +AI related data management practices (D5.2)
Legal Framework (L)	+Legal framework for PFM (L1.1)	+Network, hosting, and data center management Policies (L2.1)	+ Enforcement of paperless through the PFM legislation (L3.1) +Business continuity planning (L3.2) +Legalization of digital signatures and electronic records (L3.3)	+ Data exchange regulations/policies (L4.1) + Legality of reengineered business processes (L4.2) +FDG Legal Framework (L4.3)	+Blockchain Regulations (L5.1) +AI Regulations (L5.2) +Fiscal Data Strategy (L5.3) +Data-Driven Decision-Making Policy & Culture (L5.4)
IT Infrastructure (I)	+Availability of end user infrastructure (I1.1)	+Reliable network (I2.1) +End user IT infrastructure (I2.2) +Hosting infrastructure (I2.3) + End of support/end of life for individual components (I2.4)	+Digital signature infrastructure (I3.1) +Payment and Settlement Infrastructure (I3.2) +Digital Identity Infrastructure (I3.3)	+E-invoicing Infrastructure (I4.1) + Government-wide Messaging System (I4.2) +Data Exchange Infrastructure (I4.3) +Blockchain infrastructure (I4.4)	+Cloud/Scalable Infrastructure (I5.1) +Access to computing infrastructure for AI (I5.2) +IoT Related Infrastructure (I5.3) +CBDCs (I5.3) +Data Infrastructure (I5.4)
Governing Organizations (G)	+Organization structures for PFM (G1.1) +Supreme Audit Institution (G1.2) +Internal Audit (G1.3)	+Coordination between business and technical staff (G2.1) +Help desk/training material management (G2.2)	+Cyber security institutions (G3.1) + PFM Digitalization Strategic Management Committee (G3.2) +Secured sustainable funding (G3.3) +Political Ownership (G3.4)	+Formal data governance institutions (G4.1)	+Digital Transformation Units with (G5.1) +AI/Disruptive Technology Governance Institutions (G5.2)
Digital Skills (H)	+Trained PFM staff (H1.1)	+User IT Skills (H2.1) +Institutionalized training (H2.2) +compliance monitoring (H2.3)	+IT audit skills. (H3.1) +capacity to safely use technology. (H3.2)	+Strong Technology support (H4.1) +BPR and Change Mgt (H4.2) +digital ID (H4.3) +Data quality management skills (H4.4) +Change Management (H4.5)	+Technology management capacity (H5.1) +Disruptive technology Audit Skills (H5,2) +skills in transformative technologies planned for use (H5.3)

Managing Risks and Resiliency

- Follow a systematic and phased approach to PFM digitalization to ensure alignment with enabling environment.
- Advanced digitalization without an enabling environment increases risk exposure
- Higher stages of digitalization, when supported by strong enabling conditions, demonstrate greater resilience and adaptability to evolving risks and shocks.
- Even in digitally advanced contexts, assess the enabling environment regularly using the to identify residual and emerging risks.
- Maintain a strong focus on data quality—secure, reliable, and timely data is foundational for digital trust and effective public financial management.
- Assess your FDG practices regularly
- New risk domains are emerging with AI adoption, including algorithmic bias, data misuse, and system manipulation—necessitating updated governance frameworks.

Optimizing Workflows for Service Delivery

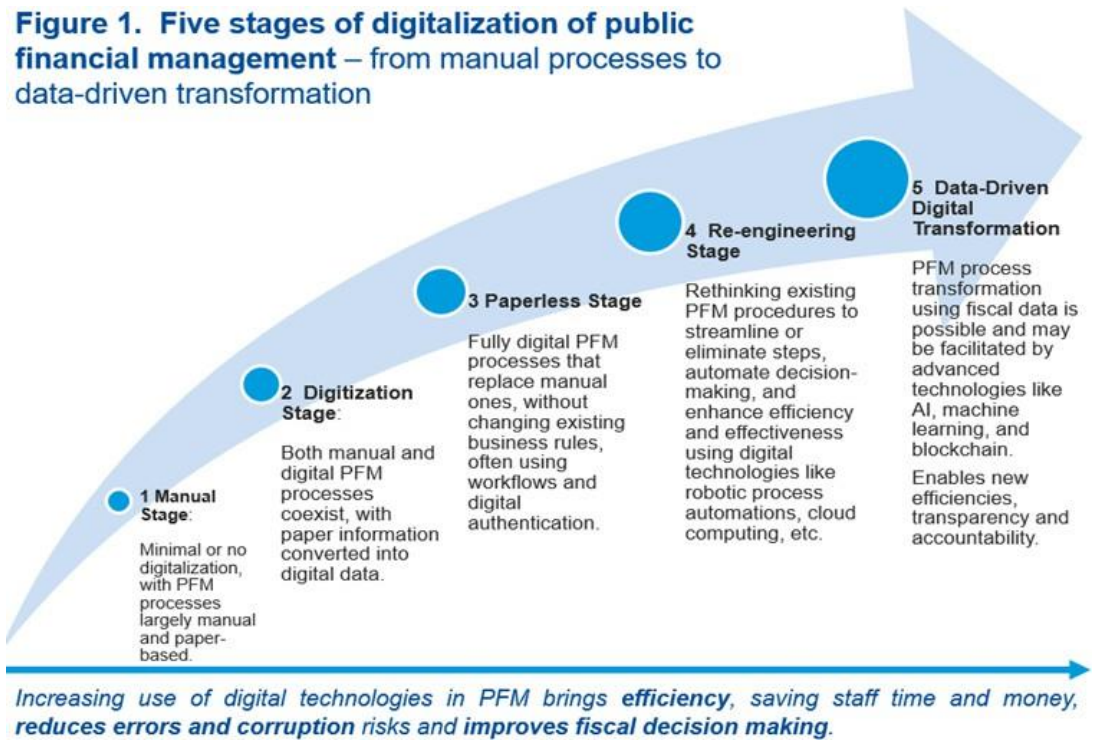


Figure 1. Five stages of digitalization of public financial management – from manual processes to data-driven transformation

Automation – levels of digitalization- what to automate ?

- Efficiency gains at each stage of digitalization

Workflow optimization should be based on the chosen stage of digitalization to manage risks

Opportunity to reengineer business process – with or without digital technology

Strong configuration of internal controls is must

- Leads to poor governance, lack of confidence in PFM Systems, unreliable budgets execution and fiscal reporting, expenditure arrears
- Undermines prudent macro-fiscal management

Workflow Optimization



Thank You