

FOR PUBLIC  
CONSULTATION



# Technical Procurement Guidance for Digital Public Infrastructure (DPI) and Services.

*Good Practices for Open, Secure, Sustainable,  
and Inclusive Procurements of Digital Solutions  
for Integrated Digital Services.*





© 2026 The World Bank  
1818 H Street NW, Washington DC 20433  
Telephone: 202-473-1000; Internet: [www.worldbank.org](http://www.worldbank.org)

Some rights reserved

This work is a product of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

### **Rights and Permissions**

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

**Attribution**—Please cite the work as follows: “World Bank. 2026. Technical Procurement Guidance for DPI and Integral Digital Services. © World Bank.”

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e mail: [pubrights@worldbank.org](mailto:pubrights@worldbank.org).

Cover photo: © Adobe Stock. Used with the permission of Adobe Stock. Further permission required for reuse.

# About us

This publication is developed by the Digital & AI Vice Presidency, WBG, with the support of the Digital Public Infrastructure & Services Umbrella Multi-Donor Trust Fund (DPI TF).

Digital Public Infrastructure (DPI) refers to the foundational digital building blocks—such as digital identity, data sharing, and digital payments—that enable governments and economies to deliver services at scale.

DPI & Services TF aims to increase the adoption and productive use of safe, inclusive, and interoperable digital building blocks and digitally enabled services. Operating as a One-World Bank effort, it mobilizes expertise across digital transformation, social protection, health, financial inclusion, agriculture, governance, and education among others; and collaborates closely with Project FASTT on fast payment systems.

The DPI & Services TF is based on three pillars:

- Knowledge: generating evidence and translating standards into practical tools;
- Action: supporting country-level DPI strategies, safe and inclusive building blocks, and sectoral digital transformation; and
- Convening: strengthening the global DPI community through peer learning, standards alignment, and digital public goods.

The work supported by the DPI TF is anchored in cross-cutting commitments **to inclusion and gender equity, human-centric design, reusability through digital public goods, safeguards**, data protection, **and evidence-based implementation**.

Building on the foundations laid by the ID4D-G2Px MDTF (2016-2026), the DPI TF is structured around three workstreams:

- The Identification for Development (ID4D) Initiative helps countries realize the transformational potential of identification systems for the Sustainable Development Goals, from foundational ID and civil registration to next-generation digital identity and trust services. Its mission is to enable all people to access services and exercise their rights by improving the inclusivity, design, and governance of ID and trust service ecosystems. Learn more at [id4d.worldbank.org](https://id4d.worldbank.org).
- The Digital Government-to-Person Payments (G2Px) Initiative transforms G2P payments to accelerate financial inclusion, women's economic empowerment, resilience, and government efficiency. It helps countries modernize their G2P ecosystems through recipient-centric frameworks and evidence-based guidance on sustainable, inclusive models. Learn more at [www.worldbank.org/g2px](https://www.worldbank.org/g2px).
- The Data Sharing workstream enables secure, interoperable, and privacy-respecting data sharing across sectors at national scale, advancing high-value use cases and inclusive benefits.

Our work is made possible thanks to the generous support of the Gates Foundation, UK International Development, French Government, Norwegian Agency for Development Cooperation, and Omidyar Network.

# Table of Contents

- Acknowledgments ..... i
- Abbreviations ..... ii
- 1. Introduction and Purpose ..... 1**
- 2. Scope and Application.....2**
- 3. Strategic Framing .....4**
  - 3.1 Strategic approach: making the case for integrated digital services.....4
  - 3.2 Principles .....5
  - 3.3 Operational approach: focus on delivery ..... 7
- 4. Procurement Strategy and Delivery Models ..... 9**
  - 4.1 “Lock-in” as a cross-cutting lifecycle risk..... 9
  - 4.2 Modular delivery model .....10
  - 4.3 Vendor managed delivery of digital solution..... 11
  - 4.4 Hybrid delivery model .....13
  - 4.5 Examples DPI and services procurement methods.....16
  - 4.6 Framework agreements for DPI and integrated digital services.....18
  - 4.7 Engaging private sector for innovation.....19
- 5. High-level Digital Solution Design and Governance ..... 22**
- 6. Bidding Documents and Evaluation..... 25**
  - 6.1 Handover strategy ..... 28
  - 6.2 References to open-source software in bidding documents ..... 28
- 7. Performance Monitoring and Contract Management.....31**
- 8. Sustainability, Ownership, and Post-Project Continuity..... 33**
- 9. Other Considerations ..... 34**
  - 9.1 Local market development, SME and start-up participation, and capacity building ..... 34

9.2 Independent oversight.....	34
9.3 Cybersecurity .....	35
<b>10. Conclusion</b> .....	<b>36</b>
<b>11. Annexes</b> .....	<b>37</b>
<b>11.1 Annex A: Update on Public Procurement Neutrality for Digital ID Solutions</b> .....	<b>37</b>
<b>11.2 Annex B: Digital Service Delivery Procurement Principles and Framework Agreement Templates</b> .....	<b>37</b>
<b>11.3 Annex C: Example Contract Clauses for DPI and Integrated Digital Services</b> .....	<b>37</b>
<b>Annex A: Update on Public Procurement Neutrality for Digital ID Solutions</b> .....	<b>38</b>
<b>Annex B: Digital Service Delivery Procurement Principles and Framework Agreement Templates</b> .....	<b>40</b>
<b>Annex C: Example Contract Clauses for DPI Procurement</b> .....	<b>55</b>

# Acknowledgments

Khalid Bin Anjum (Senior Procurement Specialist) as lead author, and Goran Vranic (Senior Digital Specialist) and Warren Smith (Director of Insight, Innovation and Impact at Posterity Global) led development of this work as co-authors. This note was developed under the guidance and supervision of Hiba Tahboub (Director and Chief Procurement Officer), Stela Mocan (Acting Director for DPI & Services), and Michel Rogy (Regional Practice Director for Digital and AI). The authors would like to thank Xiaoping Li (Lead Procurement Specialist) for his guidance throughout the work.

The authors would like to thank for inputs, advice and comments provided at various stages of the work from Alvaro Larrea (Lead Procurement Specialist), Andrew Cochran (ET Consultant), Christopher Boyd Tullis (Senior Digital Specialist), Dianne Seetahal (Procurement Specialist), Douglas Edward Fraser (Lead Procurement Specialist), Elena Corman (Senior Procurement Specialist), Irina Shmeliova (Senior Operations Officer), Isabella Hayward (Senior Digital Specialist), Jonathan Marskell (Senior Digital Specialist), Julia Michal Clark (Lead Digital Specialist), Lee Cook (Consultant), Marie Eichholtzer (Senior Digital Specialist), Milena Vuksanovic Petrovic (Procurement Specialist), Orjana Ibrahim (Senior Procurement Specialist), Peter Kusek (Lead Economist), Raman V. Krishnan (Senior Digital Specialist), Sandra V. Sargent (Senior Digital Specialist), Stephen R. Davenport (Senior Digital Specialist), Tiago Carneiro Peixoto (Senior Digital Specialist), and many other colleagues from the World Bank OPCS Procurement and Digital and AI units who participated in the meetings of the Global Working Group on Procurement and Technology Deployment of DPI and Services and internal World Bank digital procurement clinics. The authors are grateful for the valuable peer review comments received from Belita Manka (Senior Procurement Specialist), Diana Parra Silva (Senior Digital Specialist), Howard Bariira Centenary (Lead Procurement Specialist), and Joseph Huntington La Cascia (Senior Digital Specialist). Priyantha Jayasuriya Arachchi (Program Assistant) provided administrative assistance.

Washington, DC  
April 2026

# Abbreviations

<b>Abbreviation</b>	<b>Definition</b>
<b>ABIS</b>	Automated Biometric Identification System
<b>AI</b>	Artificial Intelligence
<b>API</b>	Application Programming Interface
<b>APS</b>	Accredited Procurement Specialist
<b>CQS</b>	Consultant's Qualification-based Selection
<b>DIAL</b>	Digital Impact Alliance
<b>DPG</b>	Digital Public Good
<b>DPI</b>	Digital Public Infrastructure
<b>DR</b>	Disaster Recovery
<b>EMS</b>	Education Management Systems
<b>EHR</b>	Electronic Health Records
<b>EME</b>	Early Market Engagement
<b>EU</b>	European Union
<b>FTE</b>	Full-Time Equivalent
<b>HR</b>	Human Resources
<b>IADB</b>	Inter-American Development Bank
<b>IAAS</b>	Infrastructure as a Service
<b>IC</b>	Individual Consultant
<b>ID</b>	Identification / Identity (as in Digital ID)
<b>IIITB</b>	Indian Institute of Information Technology Bangalore
<b>IP</b>	Intellectual Property
<b>IPF</b>	Investment Project Financing
<b>ITU</b>	International Telecommunication Union (United Nations)
<b>IVA</b>	Independent Verification Agent
<b>JV</b>	Joint Venture
<b>KPIs</b>	Key Performance Indicators
<b>LAs</b>	License Agreements
<b>MOSIP</b>	Modular Open-Source Identity Platform
<b>MVP</b>	Minimum Viable Product
<b>NIIS</b>	Nordic Institute for Interoperability Solutions
<b>O&amp;M</b>	Operation and Maintenance
<b>OEM</b>	Original Equipment Manufacturer
<b>OSS</b>	Open-Source Software
<b>PDOs</b>	Project Development Objectives
<b>PforR</b>	Program-for-Results
<b>PIU</b>	Project Implementation Unit

<b>PPP</b>	Public-Private Partnership
<b>PPSD</b>	Project Procurement Strategy for Development
<b>QCBS</b>	Quality- and Cost-Based Selection
<b>RACI</b>	Responsible, Accountable, Consulted, and Informed
<b>REST</b>	Representational State Transfer
<b>RFB</b>	Request for Bids
<b>RFP</b>	Request for Proposal
<b>SDG</b>	Sustainable Development Goal
<b>SI</b>	Systems Integrator
<b>SLAs</b>	Service Level Agreements
<b>SME</b>	Small and Medium-Sized Enterprise
<b>SaaS</b>	Software as a Service
<b>TOC</b>	Total Cost of Ownership
<b>TOR</b>	Terms of Reference
<b>TRC</b>	Technical Review Committee / Task Force
<b>TTL</b>	Task Team Leader
<b>U4SSC</b>	United for Smart Sustainable Cities
<b>UAT</b>	User Acceptance Test
<b>UNICEF</b>	United Nations International Children's Emergency Fund
<b>VfM</b>	Value for money
<b>WB</b>	The World Bank

# 1.

## Introduction and Purpose

Digitalizing public services at scale by applying the integrated service delivery and digital building blocks approach is central to several World Bank goals, including promoting inclusion, efficient service delivery, and resilient governance. Integrated service delivery underpins online services public institutions deliver across sectors, including energy, agriculture, health, and other sectors. The integrated service delivery and digital building blocks encompass development, deployment, integration, and maintenance of reusable software modules and digital infrastructures, requiring coordinated technical and operational efforts.

Historically, implementing digital solutions faces procurement challenges such as fragmented vendor engagement, vendor “lock-in”, limited contracting model scalability, and delays when aligning technical specifications with evolving service needs. World Bank task teams can help its borrower clients to address interoperability between diverse technologies, robust cybersecurity, review implications related to vendor lock-in, and the need for sustainability beyond project closure.

This practical guidance note is designed to help World Bank Task Team Leaders (TTLs), Accredited Procurement Specialist (APs), and borrower project teams navigate these complexities. It provides actionable good practices and tools for every stage of the procurement cycle, promoting the technical soundness of digital investments as well as making them more open, secure, sustainable, and optimized to maximize social value returns.

Digital Public Infrastructure (DPI) refers to a digitalization approach focused on implementing foundational digital building blocks designed for public benefit<sup>1</sup>. Integrated digital services—enabled by these DPI building blocks—refer to the end-to-end delivery of government services across agencies. This guidance note addresses procurement of both DPI components and integration of government services needed to deliver seamless, inclusive, and sustainable digital services. It is distinct from traditional information systems procurement in that DPI emphasizes interoperability, modularity, shared ownership, and long-term sustainability across government, rather than standalone systems serving individual agencies.

---

<sup>1</sup> “Clark, J.; Marin, G.; Ardic Alper, O.P.; Galicia Rabadan, G.A.. 2025. Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper; Volume 1. © World Bank. <http://hdl.handle.net/10986/42935> License: CC BY-NC 3.0 IGO.”

## 2. Scope and Application

This practical guidance outlines good practices that can be shared with borrowers and the ecosystem—including the private sector—for World Bank-funded operations<sup>2</sup>, whether financed through Investment Project Financing (IPF) or Program-for-Results (PforR). The guidance is not mandatory but rather serves as a resource for teams to tailor to their specific contexts.

### Box 2.1: Note on Guidance Applicability

Much of the procurement terminology in this guidance—such as Project Procurement Strategy for Development (PPSD), specific procurement methods, and contract forms—relates specifically to the World Bank Procurement Framework under IPF operations. For PforR operations, which use borrowers' procurement systems, national procurement laws may differ. In PforR contexts, teams should treat the principles and good practices in this guidance as advisory benchmarks, adapting them to the Borrower's national procurement framework. The core principles of outcome-based, technology-neutral procurement, and the strategic considerations for DPI, remain relevant across both financing instruments.

This guidance discusses two types of “lock-in” risks that require different mitigation strategies:

- i. *Vendor lock-in*, which refers to commercial and contractual dependence on a specific supplier, making it costly or difficult to switch providers.
- ii. *Product lock-in*, which refers to technical dependence on a specific platform, product, or technology stack, regardless of which vendor supplies it.

Both risks must be assessed and mitigated throughout the procurement lifecycle—from strategy and requirements through evaluation, contracting, and implementation—as they affect long-term sustainability, cost, and government control over digital assets.

---

<sup>2</sup> Systems and components may include digital building blocks and integrated service delivery, such as electronic health records (EHR) systems, education management information (EduMIS), civil registration and vital statistics (CRVS) systems, integrated services for businesses and investors, and other sectoral digital solutions in energy, agriculture, health, and other sectors.

The guidance outlines the key stages of the procurement cycle: needs assessment, strategy, specification, bidding, evaluation, contracting, and implementation. These also align with the World Bank operations lifecycle. Teams are encouraged to use this guidance to ensure their procurement processes align with global best practices and World Bank policy.

To further strengthen implementation and learning, the World Bank is spearheading a peer support network—a community of practitioners—through the Global Working Group on Procurement and Technology Deployment of DPI and Services. This network fosters continuous exchange among World Bank TTLs, procurement specialists, client counterparts, private sector representatives, the digital public goods community, and other development partners, helping to identify practical solutions, address common challenges and promote collaborative problem solving. Despite facing outward and being applicable beyond the scope of World Bank operations, the Global Working Group will provide feedback for continuous improvement of this guidance and evolve into a platform to showcase successful projects, demonstrating the benefits of applying and advancing this guidance in diverse operational contexts.

# 3.

## Strategic Framing

At the outset of a project engagement, it is important to establish a good strategic framing for digital building blocks and integrated digital services. All subsequent decisions and activities must tie back to this framing and be able to demonstrate significant and measurably successful outcomes.

### 3.1 Strategic approach: making the case for integrated digital services

A compelling case for integrated digital service delivery leveraging reusable digital building blocks starts by demonstrating strategic alignment with partner countries' national priorities in areas such as digital government transformation, economic development, resilience, inclusion, and trust. The goal is not “more technology” but better outcomes in terms of end-to-end, individual and business-centric services being delivered seamlessly across agencies and levels of government. This improved service delivery is enabled by a shared set of interoperable building blocks; for example, digital identity, e-payments, data exchange systems, messaging/notifications, interconnected registries through data catalog/meta-register. This “building blocks” approach enables faster delivery, consistent user experience, and lower long-term cost by reusing common capabilities rather than repeatedly rebuilding them for each sector or ministry.

A coordinated and integrated service delivery approach involves:

- Integrating national and subnational/municipal strategy that explicitly prioritizes cross-government/sector service journeys and digital building blocks as public value assets.
- Investment in inclusive, scalable, and interoperable infrastructure, designed around open standards and data exchange interfaces so components can evolve independently.
- Promotion of human rights and digital trust through privacy-by-design, security-by-design, and accountable governance.
- Strengthening private sector engagement and the innovation ecosystem to bring new capabilities, delivery models, and implementation capacity.
- Establishing enabling regulation and a business-friendly environment that supports competition, interoperability, and sustainable digital markets.

- Measuring results and sharing best practices to accelerate adoption and continuous improvement.

## 3.2 Principles

**Core Principle—Outcome-Based and Technology-Neutral Procurement:** All procurement activities under this guidance are anchored in outcome-based and technology-neutral principles. This means specifying what the digital solution must achieve in functional and performance terms—such as interoperability, scalability, security, and user-centricity—rather than prescribing specific products, vendors, or technologies. This principle enables competition, supports innovation, improves value for money, and reduces vendor lock-in risk. This principle should consistently guide procurement decisions across the entire lifecycle, from strategy and defining requirements through evaluation, contracting, and implementation.

The following recommends other high-level principles to govern and optimize decision making before, during, and after DPI and integrated digital services procurement:

- **Understand and meet users’ needs through service design:** Design integrated digital services around people’s needs—not government structures. Engage users—whether individuals, businesses, public sector workers, or other groups—early and continuously through research, testing, and feedback. Prioritize accessibility and usability for all users, including persons with disabilities and those in rural or underserved communities. Use plain, contextually relevant language, where possible, and ensure multilingual inclusivity to respect and reflect specific countries’ cultural diversity and heritage.
- **Ensure inclusive and equitable access:** Integrated digital services should benefit everyone, regardless of their location, ability, or digital literacy. Apply digital inclusion strategies, and offer digital support assistance. Promote access equity by designing for the most vulnerable from the outset. Attempt to bridge digital divides by supporting local contexts, languages, and needs.
- **Be open by default:** Transparency, collaboration, and openness in integrated digital service delivery should be normal. Use and publish open data wherever possible and as appropriate. Equal consideration should be given to open source and proprietary software when evaluating options. Openly share source code, standards, digital public goods (DPGs) and DPI digital building blocks, and learnings and implementation insights to enable reuse and reduce duplication.
- **Build trust by being secure and respecting privacy by design:** Develop secure and privacy-respecting digital services to earn and maintain public trust. Embed privacy and data protection from the outset (“privacy by design”). Follow and comply with relevant data protection regulations and international standards. Borrowers should be transparent about data use and provide individuals with control over their data.
- **Understand digital supply ecosystem:** Base decisions on what to procure and how to procure on clear understanding of what is available—reusable DPI and DPGs, cloud-based software and hosting infrastructure, digital delivery capabilities—and how these align to these principles.
- **Procure sustainably and for resilience:** Buyers should: (i) design their DPI and integrated digital services projects with long-term environmental, social, cultural, and economic sustainability, positive impact, and resilience; (ii) create long-term plans on how to increase their digital

service solutions sustainability across their entire lifecycle; (iii) assess and manage total cost of ownership (TCO) across the full lifecycle—covering development, licensing or subscription costs, customization, integration, operations, maintenance, upgrades, security, and exit/transition costs—irrespective of whether solutions are based on open-source or proprietary software; (iv) deliberately support the development of local digital ecosystems—including local and regional firms, integrators, MSMEs, and skills—to enable effective operation, ongoing maintenance, and continuous improvement of digital services over time.

- **Integrate and adapt:** Buyers should:
  - i. Ensure that new technologies work with existing digital solutions, legacy solutions, processes and infrastructure in their organizations, without limiting their ability to adapt to future demands, ensure data portability, or upgrade systems.
  - ii. Use integration planning to minimize risk to infrastructure by identifying any compatibility gaps in new technologies.
  - iii. Minimize single points of failure using systems that enforce built-in redundancy of services.
  - iv. Promote technology project or program flexible and interoperability by following commonly accepted standards principles and using open standards that meet their requirements
  - v. Use Representational State Transfer Application Programming Interfaces (REST APIs) for integration where possible.
  - vi. Consider what skills and capabilities their organizations need to deliver and support the products or services they will reuse, buy and build.
- **Consider cloud first:** When procuring or renewing DPI digital building blocks and integrated digital services, buyers should:
  - i. Fully evaluate potential public cloud solutions first before considering other options.
  - ii. Continually revalidate cloud hosting strategies, investment cases, and legacy migration plans to select the right cloud computing services.
  - iii. Be clear about how to manage vendor and technical dependencies to an acceptable level.
  - iv. Follow specific countries' policy and guidance on offshoring and data residency.
- **Configure rather than customize:** Buyers should decide whether commercial off-the-shelf (COTS) software meets their functional and non-functional requirements and should use COTS software as intended, avoiding or minimizing modifications and customizations. Borrowers should aim to only configure COTS software settings to ensure receipt of ongoing vendor support when new versions are released.
- **Measure what matters:** Buyers should use meaningful quantitative and qualitative data to assess outcomes, not just outputs, of their DPI and integrated digital services projects. This includes setting measurable goals tied to user value and public benefit, which should feed procurement evaluations and be proactively monitored during implementation. Buyers should collect and publish service performance data to improve transparency and learning and monitor not only technical performance but user satisfaction and equity repercussions.

### 3.3 Operational approach: focus on delivery

A thorough needs assessment represents the foundation of successful digital procurement. The focus shifts to implementation once having established the strategic framing and case for adopting digital building blocks and integrated service delivery. To translate strategic vision and intent into practical action through procurement and contracting, it is fundamental to start by researching and analysing peoples' needs, or problem identification. Teams should begin by defining what outcomes the system must achieve in terms of enabling integrated digital services using functional and performance terms, rather than specifying any specific product or technologies. This approach encourages a focus on purpose, and supports greater innovation, competition, and value for money (VfM).

Practical steps include:

- **Assessing needs** based on research with end users to identify essential system functions.
- **Mapping and redesigning procedures** and processes to identify pain points, dependencies, and integration needs across agencies.
- **Specifying scalability and interoperability;** for example, progressive compliance with or alignment to standards.
- **Considering lifecycle costs,** including total cost of ownership, obsolescence risk, exit and transition costs, and decommissioning.
- **Avoiding “gold-plated” specifications** that exceed actual needs, and overspecifications that stifle innovative solutions for the problem at hand.
- **Applying agile delivery as a core implementation principle.** Prioritize a minimum viable set of digital building blocks and high-impact integrated services, then iterate based on user feedback, operational learning, and policy evolution.
- **Avoiding technology bias.** State functional outcomes, not brand names or proprietary products.
- **Defining acceptance criteria** early. For instance, focus on performance metrics such as user satisfaction, authentication success rate, and system uptime, which can help lower costs, improve quality, and broaden vendor participation.<sup>3</sup>

When reviewing Terms of Reference, teams should be aware that both over- and under-specification carry risks. Over-specification—prescribing specific technologies, products, or excessively detailed technical requirements—can stifle innovation, limit competition, and increase costs. Under-specification—using overly generic or vague outcome statements—can create ambiguity during evaluation and implementation, making it difficult to hold vendors accountable. The recommended approach is to define clear functional and performance requirements with measurable acceptance

---

<sup>3</sup> A standard set of performance metrics and functional requirements can be developed—especially for common systems like digital ID, electronic health records (EHR), and education management systems (EMS)—across countries to be adapted as needed. The UN ITU U4SSC guidance recommends scientifically rigorous approaches to measuring DPI benefits, which demand continuous measurement, best practice sharing, and structured learning. Systematic monitoring is critical to assess operational performance and broader societal outcomes. To this end, Key Performance Indicators (KPIs) for DPI should encompass measures such as system adoption rates, demographic inclusion, service uptime, incident and tampering reports, cost-efficiency assessments, and socio-economic impacts such as reduction in service wait times or increased public access to essential services.

criteria, while leaving the technical approach and solution design to the vendor's expertise. For example, rather than specifying a particular database technology, specify data throughput, query response times, scalability targets, and interoperability standards that the solution must meet.

It is important to note that the above points relate to post-procurement contracted service delivery, so anticipating this continuous measurement, best practice sharing, and structured learning (the outputs) as part of your procurement and contract design (the inputs) will be critical for successful outcomes.

Together, the strategic framing and needs assessment will feed directly into development of the procurement strategy and approach.

## 4.

# Procurement Strategy and Delivery Models

Choosing the right procurement strategy is vital. Teams should weigh the pros and cons of modular versus vendor-managed delivery approaches, as well as a hybrid approach:

- **Modular delivery model** promotes flexibility, competition, adoption of “best of breed” solutions, and local industry participation, but requires strong integration management and client capacity for project management.
- **Vendor-managed delivery of the digital solution** simplifies management and integration for the government client but increases dependency on a single supplier and risk of vendor lock-in, and can escalate costs for upgrades.
- **Hybrid delivery model** combines vendor managed delivery of the core system with separately procured modules or add-ons, balancing integration and flexibility while enabling phased innovation and local ecosystem development.

A procurement strategy goes beyond choosing between modular, vendor-managed or hybrid delivery models; it defines how the solution aligns with national digital transformation priorities, embeds specific policy objectives (such as regulatory compliance, digital sovereignty, data protection, cybersecurity, and support for local entrepreneurship), and ensures interoperability through mandated standards and architectural requirements. It also clarifies how procurement will be structured—whether components will be bundled into a single package or divided into multiple lots that encourage competition and local participation—and sets out long-term maintenance expectations, upgrade pathways, financing mechanisms, and hosting arrangements, including whether hardware will be procured, cloud services provided by the government, or a Software as a Services (SaaS) model adopted. Within the World Bank procurement framework, the strategy must also articulate decisions on procurement category, selection method, market approach, contract type, and the use of framework agreements and other standard procurement documents (SPDs), explaining how each choice affects risk allocation, market engagement, implementation responsibilities, and overall value for money. All these dimensions are addressed in detail in the forthcoming sections of this guidance.

### 4.1 “Lock-in” as a cross-cutting lifecycle risk

Lock-in—whether commercial, contractual, or product—is not a risk to be addressed at a single stage of the procurement lifecycle but a cross-cutting strategic concern that must be systematically

identified and mitigated from the earliest procurement planning through implementation and post-project operations. Regardless of which delivery model a borrower selects (modular, vendor-managed, or hybrid), a vendor relationship will almost always exist unless the government has full in-house capacity. The focus should therefore be on designing procurement strategies, contract structures, and governance mechanisms that preserve government control, enable portability, and allow the competitive replacement of components or providers over time.

Key mitigation measures include:

- Mandating alignment to standards and interoperable interfaces from the requirements stage.
- Requiring comprehensive documentation and knowledge transfer throughout the contract.
- Embedding data ownership and data portability provisions in contracts.
- Building in exit and transition planning as a contractual obligation from the outset.
- Distinguishing between more reversible dependencies (such as infrastructure or tooling choices) and less reversible architectural decisions (such as identity frameworks, data models, and core security controls) that may significantly constrain future options.

Teams should encourage borrowers to document conscious trade-offs when dependencies are introduced and to assess the reversibility of architectural decisions at each procurement stage. For example, an earlier ID4D Procurement Guide<sup>4</sup> published emphasizes that using open-technology standards and globally accepted interoperability practices allow governments enough flexibility to easily upgrade critical system components with minimal vendor dependency, minimizing longer-term costs.

## 4.2 Modular delivery model

The United Nations International Children’s Emergency Fund (UNICEF) Digital Public Goods Toolkit<sup>5</sup> describes modular procurement and contracting as an approach that breaks large digital programs into smaller, self-contained implementation elements, which are bought and delivered in short, iterative cycles with clearly defined outcomes and acceptance criteria<sup>6</sup>. The key is to choose module sizes that align with both the component and the overall multiple-vendor ecosystem that borrowers want to build.

This approach aligns commercial structures with agile and user-centric delivery models, emphasizing flexibility, the use of open standards and open interfaces, and iterative feedback rather than monolithic, long-term contracts. In essence, the technical modularity of integrated service delivery approach is mirrored by modular procurement and contracting structures, which enable swapping out underperforming components or vendors without having to rebuild entire systems<sup>7</sup>.

---

<sup>4</sup> Procurement Guide and Checklist for Digital Identification Systems, accessible on [https://id4d.worldbank.org/procurement\\_guide](https://id4d.worldbank.org/procurement_guide).

<sup>5</sup> [Digital Public Goods Toolkit](#) (UNICEF, 2023)

<sup>6</sup> On sizing modular contracts, the UNICEF toolkit states that this will depend on overall budget, the nature and scale of specific programs and projects, and the ecosystem needs at a particular stage of development. They provide an illustrative example of a medium-sized informational website project where Borrowers might employ contracts no smaller than \$60,000, which would allow multiple vendors while still providing enough budget room for vendors to deliver without squeezing margins so much that quality suffers.

<sup>7</sup> [Digital Public Infrastructure and Development: A World Bank Group Approach](#) (2025)

Embarking on a path towards modular procurement and contracting requires borrowers to have sufficient technical and commercial capacity and forward planning to proactively manage diverse, integrated vendor ecosystems and the associated contracts and vendor relationships. The borrower retains full responsibility for overall project management and delivery of the digital solution, while vendors are accountable only for specific modules and integration services for which they are contracted. Traditionally, contracting authorities are likely to have outsourced such capabilities fully to systems integrators (SIs), so wholly or even partially insourcing these responsibilities requires careful consideration and capacity planning, which should feature as part of strategic contextual framing and the Project Procurement Strategy for Development (PPSD).

More modular approaches to procurement and contracting are endorsed across modern digital governments as essential to reducing delivery and vendor lock-in risks, improving agility, and widening supplier participation.

In lower-capacity contexts, borrowers considering modular approaches should ensure that complementary architectural support and independent assurance are in place before procurements begin. This may include engaging an independent architecture advisor or Technical Review Committee during project preparation, developing an early architecture blueprint and roadmap, and securing dedicated technical assistance, including through World Bank trust funds or grant facilities, to help manage multi-vendor coordination. The DPI Maturity Assessment framework can help determine whether the borrower has sufficient capacity for modular delivery or whether additional support mechanisms are needed.

**Table 4.1: Pros and cons of modular delivery approach**

Pros	Cons
Principles- and standards-based governance: Borrowers can set “the rules of the game” based on interoperability, integration, and architectural independence.	Higher architecture and governance workload: Borrowers must define the architecture, interfaces, and integration rules (or procure strong independent assurance support).
Reduced delivery risk: smaller increments make it easier to correct course and avoid catastrophic failures.	Integration accountability can blur: “who owns end-to-end outcomes?” must be explicitly managed (for example, through or in conjunction with a system integrators or government-led integration (see ‘Hybrid procurement’).
Better competition and value: you can source specialists per module and replace underperformers.	Procurement/contract overhead: more vendor management, more contract administration.
Less lock-in, if interfaces are well-governed: modules can be recompeted; better leverage of open standards.	
Faster learning cycles: aligns well with agile/iterative delivery and evolving policy needs.	

### 4.3 Vendor managed delivery of digital solution

Vendor managed delivery and contracting is an approach where government allows a single prime supplier (or consortium) to take end-to-end responsibility for delivering a defined outcome, typically covering solution design, build/configuration, systems integration, testing, rollout/change management, and often operations/support under one contract with clear performance obligations.

The vendor managed delivery can accelerate delivery and simplify accountability, but for digital building blocks it works best as “vendor delivery of a modular, standards-based platform”. The borrower can evolve, compete, and govern the infrastructure over time rather than becoming

dependent on a single vendor. This approach can be appropriate when speed and single-point accountability matter, but it should be structured to preserve long-term public value and reduce delivery risk by:

- Specifying outcomes, not a predetermined product (service levels, user journeys, policy and inclusion goals), and using data and lifecycle thinking to manage procurement end-to-end.
- Using fit-for-purpose procurement strategies—such as early market engagement (EME), risk allocation, or supplier performance management—rather than “one-size-fits-all” contracting.
- Building in transparency, integrity, and competition safeguards, such as clear evaluation criteria, auditability, conflict-of-interest controls.
- Avoiding “black box” delivery by requiring open standards/interoperability, documentation, and knowledge transfer, which are common recommendations in modern digital procurement reform and innovation-friendly procurement.

To structure turnkey approaches to align with these principles, borrowers should consider:

- Requiring modular architecture, open and industry-standard Application Programming Interfaces (APIs), portability, and no proprietary lock-in; for example, use government-owned interfaces/specifications, suppliers must publish/maintain API documents, and creating clear exit plans.
- Reusing and re-configuring (not customizing) existing digital building blocks and digital public goods (DPGs), and contract for configuration/integration rather than bespoke reinvention.
- Making governance and safeguards contractual, including security-by-design, privacy and rights protections, audit logs, resilience, and inclusive access.
- Using phased delivery with acceptance gates; for example, discovery, minimum viable product (MVP)/alpha, scale/beta, with payments tied to verified milestones and outcomes, not just activities.

**Table 4.2: Pros and cons of vendor-managed delivery model**

Pros	Cons
Single point of accountability: one vendor owns delivery, integration, and (often) service levels, which simplifies the implementation governance.	Vendor lock-in risk (technology plus know-how): switching costs can be high if interfaces, data models, or operations are proprietary, and knowledge is not systematically transferred to Borrower throughout the life of the contract.
Speed when requirements are stable: works well if scope is well-defined and the market offers mature “productized” solutions.	Change vulnerability: change requests can be expensive/slow; incentives often favor “deliver to specification” over iterative improvement.
Lower internal capability burden (initially): less need for deep in-house architecture / product management at the start.	“Big-bang” integration risk: if delivery follows a “waterfall” methodology, end-to-end integration issues may surface late (during acceptance testing), increasing delays and likelihood of disputes.
	Potentially harder ecosystem participation: local small and medium-sized enterprises (SMEs) and specialist providers can be crowded out by the SI’s stack, unless specific ecosystem participation interventions are specified and proactively managed by Borrowers.

## 4.4 Hybrid delivery model

A hybrid approach combines modular and vendor-managed delivery approaches. Hybrid approaches seek to balance integration and accountability, through the core vendor delivery model contract, with competition, flexibility, and phased innovation. The hybrid approach uses a modular approach and solutions that can evolve over time and grow local vendor ecosystems.

Early contextual research and analysis is critical to develop the plan for a hybrid approach as part of the procurement strategy, including how the hybrid profile will be expected to evolve over time as internal client capabilities and capacities are built. This may happen following investment in new skills and ways of working, as governance arrangements are rolled out, with support from the systems integrator (SI) through knowledge transfer, among other reasons.

The specific pros and cons of both vendor delivery and modular approaches are broadly applicable with the hybrid approach. A focus on building client capabilities is central to the hybrid approach, including establishing principles- and standards-based governance to set “the rules of the game” based on interoperability, integration and architectural independence of the digital building blocks.

**Table 4.3: Pros and cons of the hybrid approach**

Pros	Cons
Balance accountability and flexibility: one party can be accountable for integration, while digital building blocks remain “hot swappable” (providing technical and commercial flexibility has been consciously designed into procurements and contracts).	Governance complexities remain: Borrowers still need strong architecture, interface standards, and performance management.
Accelerate delivery using reusable components: Borrowers can potentially stand-up digital building blocks faster.	Risk of “modular in name only”: a SI may bundle digital building blocks into a de facto monolith unless contract management specifically prevents it.
Supports local ecosystem prosperity: digital building blocks can be sourced competitively while the SI leads or assists with coordination.	Commercial complexity: allocating liability between digital building block vendors and the SI requires careful contract design, governance and “intelligent client” capabilities within Borrower countries.
Path to sovereignty: providing contracts requires open interfaces, source access, and skills/knowledge transfer.	

In summary, the procurement strategy should balance competition, manageability, and sustainability. The choice—modular, vendor managed, or hybrid approach—should be guided by market conditions, technical readiness, institutional capabilities and capacities, and long-term interoperability needs (see Box 4.1).

### Box 4.1. Selecting the appropriate delivery model

The choice between modular, vendor-managed, and hybrid approaches should be informed by a structured assessment of the:

- Borrower’s institutional capacity for managing multiple vendors, architectural governance, and contract administration.
- Depth and competitiveness of the local and regional market.
- Complexity and interdependence of the digital building blocks being procured.
- Government’s risk appetite and political context.

In practice, very few borrowers currently have the full capacity to manage a purely modular approach, and most implementations will involve some form of hybrid or vendor-managed delivery. Where borrower capacity is limited, teams should consider minimizing the number of contracts and ensuring strong independent assurance and architectural advisory support are in place before procurements commence.

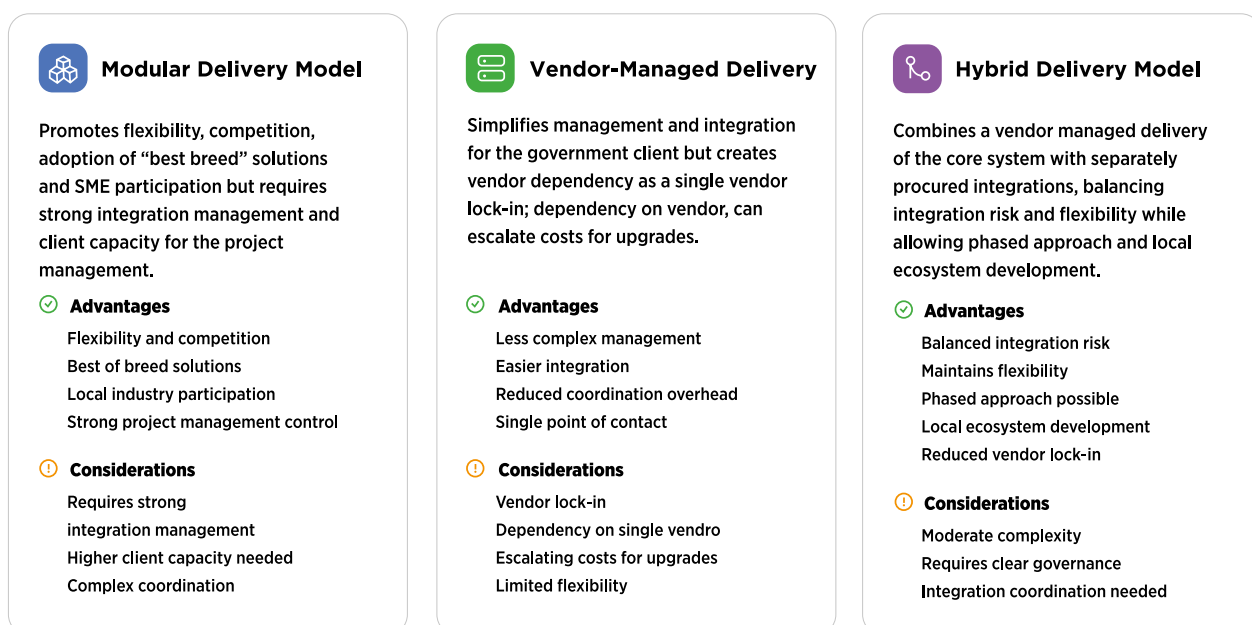
Table 4.4 summarizes key considerations for developing an effective procurement strategy, which will support analysis of vendor managed, modular and hybrid approaches:

**Table 4.4: Key considerations for selecting modular, vendor, and hybrid approaches**

Key considerations	Explanation
Alignment with Project Development Objectives (PDOs)	This ensures procurement decisions contribute directly to achieving intended outcomes and delivering VfM rather than focusing only on lowest price. Procurement objectives should be SMART (Specific, Measurable, Achievable, Relevant, Time-bound) and aligned with project goals.
Strategic assessment of context and capacity	<p>Teams must assess the operating environment and the Borrower’s capabilities. This should include:</p> <ul style="list-style-type: none"> <li>• Operational context (political, economic, social, technological, legal, environmental factors – PESTLE).</li> <li>• Borrower capacity such as experience, governance, resources, and contract management capability.</li> </ul> <p>This assessment helps determine whether the organization can realistically manage the chosen procurement approach or need additional support.</p>
Market research and analysis	<p>Understanding how the market works in each context is essential. Market analysis identifies:</p> <ul style="list-style-type: none"> <li>• Number and type of potential vendors;</li> <li>• Level of competition; and</li> <li>• Pricing structures and capacities.</li> </ul> <p>This research and analysis will ensure the procurement approach attracts suitable bidders and reduces the risk of failed or non-competitive procurement. It will also help to ensure that contract lots are designed to align with the target market.</p>
Supply positioning and supplier behavior	<p>Each contract should be positioned according to risk and value. This helps determine:</p> <ul style="list-style-type: none"> <li>• How much effort and analysis are needed; and</li> <li>• Whether the contract is strategic, critical, or routine.</li> </ul> <p>Supplier preferencing is also used to anticipate how suppliers are likely to behave and how attractive the buyer is to them.</p>

Stakeholder analysis	Key stakeholders should be identified, along with their interests, power, and influence. Their needs should be prioritized and managed through a stakeholder engagement plan to avoid conflicts and ensure buy-in.
Procurement risk analysis	Risks such as limited competition, weak capacity, market instability, or governance issues should be assessed early. A risk management plan should outline mitigation measures to protect project delivery and VfM.
Design of the procurement approach	<p>The strategy must define five core elements:</p> <ol style="list-style-type: none"> <li>1. Requirements – clear, outcome- and performance-based technical requirements specifications;</li> <li>2. Contract strategy – type of contract including the use of framework agreement, slice-package for procuring multiple lots, , pricing mechanism, and risk allocation;</li> <li>3. Selection methods – open, limited, or direct selection;</li> <li>4. Evaluation methods – including Rated Criteria (quality, sustainability, innovation), and weighting to be applied for quality and innovation; and</li> <li>5. Contract management approach – KPIs and performance monitoring.</li> </ol> <p>These elements ensure the approach is fit-for-purpose and aligned with market realities.</p>
Evaluation of options and recommendations	Multiple procurement options should be developed and assessed against procurement objectives. The preferred option is selected only after comparing how well each option delivers VfM, manages risk, and supports project outcomes.
Contract management and performance	Procurement does not end at contract award. Effective contract management, including KPIs, incentives, and monitoring mechanisms, is essential to ensure suppliers deliver what was promised and VfM is realized in practice.
Proportionality and fitness-for-purpose	The level of analysis and details must be proportionate to the project’s risk, value, and complexity. High-risk or high-value contracts require deeper analysis, while low-risk activities can follow simplified arrangements.

**Figure 4.1: High-level Models for Digital Solution Delivery for DPI and Services**



Procurement strategies, following current World Bank procurement policies and procedures, aim to determine the most suitable and effective procurement methods, in this case for implementation of digital building blocks and integrated service delivery, ensuring value for money, transparency, and fit-for-purpose approaches. This process involves analysing market conditions through desk and

proactive early market engagement (EME), as well as beneficiary implementation capacity and the technical nature of each component to define an optimal packaging and procurement approach.

**Table 4.5: Examples of implementation approaches**

Example	Context & Objective	Market Analysis Approach (Desk Research + EME)	Implementation Capacity Considerations	Resulting Packaging
1. Digital ID	Implement a foundational digital ID system to support multiple government services.	Desk research to map global ID standards and vendor ecosystems; EME with major identity providers and local ICT firms to validate feasibility, integration requirements, and cost drivers.	Beneficiary has limited digital integration capacity; requires strong vendor support for onboarding, testing, and security hardening.	Single procurement lot for the core digital ID platform + separate lots for ABIS and civil registry integration and onboarding services, enabling modular approach and competition on the systems integration layer.
2. Government Data Exchange Platform	Establish a national data exchange layer.	Desk review of interoperability frameworks; EME workshops with API platform vendors, cloud providers, and local software firms to identify standards, migration constraints, and innovation opportunities.	Beneficiary has moderate technical capacity but limited experience in API governance; requires capacity-building embedded in contracts.	Modular packaging: (1) Data Exchange Platform; (2) API governance framework + training; (3) Priority service integrations (Health-ID, Social Protection-Payments), allowing phased deployment.
3. Integrated digital services for businesses	Digitalize and harmonize multiple services for businesses and investors into a unified service delivery workflow.	Market research on content and workflow management systems; Targeted EME with local vendors.	Beneficiary has strong program-management capacity but limited digital capabilities; requires adaptable configuration rather than custom builds.	Hybrid approach: Core content and workflow management system procured as a configurable SaaS solution, while customization, integration, and change management support are procured in separate lots to encourage local participation.

## 4.5 Examples DPI and services procurement methods

Table 4.6 presents example procurement methods for implementing DPI digital building blocks and digital services. Not all packages are required, nor should they be procured and contracted separately. As part of developing the PPSD, borrowers should consider how relevant packages can be logically grouped based on their context, while ensuring alignment with World Bank core procurement principles. Such grouping will also support considerations for procurement lots and framework agreements, all of which should be informed by EME.

**Modern digital solutions procurement can no longer rely on traditional “goods-based” approaches that assume vendors will supply or specify on-premises infrastructure.** In the cloud era, deployment models vary—such as government-mandated IaaS, vendor-provided SaaS, or other options when using two-stage RFP, with each requiring a different procurement category and method, typically within Non-Consulting Services rather than goods. This guidance therefore emphasizes clearly stating the intended deployment model upfront, aligned with cloud-procurement guidance developed in parallel, which helps governments choose and structure the appropriate cloud-based solutions approach.

**Table 4.6: Examples of procurement methods for implementing DPI solutions and integrated service delivery**

Package	Procurement category	Selection/ market approach	Contracting Arrangement	Threshold / comment
User research, user needs assessment and design of implementation approach	Consulting Services	RFP – QCBS or CQS	Single contract	Can be packaged together with the legal and institutional assessment
Legal and institutional assessment	Consulting Services	RFP – QCBS or CQS	Single contract	
“Pre-selection of vendors” for implementing software modules of DPI and digital services	Non-Consulting Services	RFB or RFP	Framework Agreement + call-offs	
Modular approach - agile implementation, where quality of teams, speed, and iterative delivery are critical.	Non-Consulting Services	RFP rated criteria	Framework Agreement + call-offs	
Implementation/customization of the digital building blocks and integrations of services following the agile approach, including over an existing open source or proprietary solution	Non-Consulting Services	RFP or RFB	Single contract or Framework Agreement + call-offs	
Equipment (computers, biometric or card readers, printers, enrollment kits, etc.)	Goods	RFB or RFQ	Single contract	Can be packaged together with the implementation of the card production system
Training and capacity development <sup>8</sup>	Consulting Services	RFP – QCBS or IC	Single contract for firm or IC	
Software-as-a-service license (e.g., liveness check for e-KYC)	Non-Consulting Services	RFQ or Direct Selection	Single contract	Direct selection can be applied when appropriate
Infrastructure- or platform-as-a-service	Non-Consulting Services	RFP or RFB	Single contract	
Independent cybersecurity audit	Consulting Services	RFP – QCBS or CQS	Single contract	If appropriate, implementation of (some) measures can be included in this package
Maintenance of the implemented solution/module	Non-Consulting Services	RFP/RFB or Direct Selection	Single contract	
Off-the-shelf service subscriptions (e.g. API calls, AI services subscriptions)	Non-Consulting Services	RFQ/Shopping	Single contract	

<sup>8</sup> For training and capacity building subject to procurement.

While this guidance note emphasizes Non-Consulting Services and Consulting Services as primary procurement categories for DPI and digital services, goods-based procurement may still be appropriate for hardware components such as biometric enrollment devices, identity card production equipment, and off-the-shelf equipment. That said, goods-based procurement of information systems may not always be the most suitable approach for DPI and integrated digital services contexts, as such approach can make it more difficult to address the full range of services needed to develop and integrate, nor to address agile implementation approaches and ongoing operational requirements.

## 4.6 Framework agreements for DPI and integrated digital services

Framework agreements provide a structured procurement mechanism particularly well-suited to DPI and integrated digital services, where requirements may evolve over time, multiple service packages may be needed, and agile delivery models call for rapid mobilization of specialist teams and resources. Under a framework agreement, borrowers conduct a primary (first-stage) procurement to pre-qualify a panel of vendors against defined criteria, and then issue call-off contracts (secondary procurement) for specific work packages as needs arise.

Framework agreements are suitable when all of the following factors apply:

- The project involves multiple, phased procurement packages sequenced over project lifecycle.
- Agile delivery is planned and requirements will be refined iteratively.
- The market includes a sufficient number of qualified vendors to sustain meaningful competition at the call-off stage.
- The borrower has, or can develop, sufficient capacity to manage call-off processes.

Framework agreements may not be appropriate when one or more of the following factors apply:

- The market is too narrow to sustain competition across the panel.
- The scope is well-defined and a single contract with clear milestones is more efficient.
- The risk of over-concentration is high (causing a small number of pre-selected vendors to capture the vast majority, or all, work).
- The borrower lacks capacity to manage multiple call-off processes.

The use of framework agreements must comply with the World Bank Procurement Regulations, including PPSD justification, open and competitive panel selection, clear call-off procedures, and World Bank review. See Annex B for a practical template.

## 4.7 Engaging private sector for innovation

The market for DPI, digital systems, and service design and delivery capabilities differs from traditional sectors. Competition in some cases involves authorized resellers, SIs, and Original Equipment Manufacturers (OEM), while others cases require open-source software components as an input for implementing a DPI solution. To ensure a fit-for-purpose approach, engagement with the private sector should begin early during WB project design; for example; through focus groups with private sector associations. During implementation, borrowers should also apply constructive, incremental EME to map their needs with supplier structures, evaluate interoperability options and alternatives, and understand local integration capacity. These insights should inform the PPSD, ensuring that specifications and procurement strategy align with actual market conditions and support fair competition.

Table 4.7 provides a detailed overview of good practices for EME in implementing DPI and integrated service delivery, summarizing key actions borrowers should take to align with WB EME requirements. EME can help borrowers determine the best approach—modular, vendor-managed, or hybrid digital solution delivery, as well as procurement methods and contracting approaches. EME can also help broaden contractor participation, identify potential innovative alternatives and reduce vendor lock-in risk.

**Table 4.7: Do’s and don’ts for early market engagement (EME)**

Do’s	Don’ts
<ul style="list-style-type: none"> <li>- <b>Plan and document EME in the PPSD</b>, including objectives, format, timeline, and how results will inform the procurement approach.</li> <li>- <b>Conduct EME early—during project preparation—and update findings throughout implementation.</b></li> <li>- <b>Use transparent formats such as open briefings, RFIs, questionnaires</b>, and structured bilateral meetings with clear protocols. Record and publish appropriate summaries while protecting confidential information.</li> <li>- <b>Share only non-confidential, high-level information equally</b> with all market participants, ensuring transparency and auditability.</li> <li>- <b>Use neutral, functional language in all communications</b> to maintain fairness and avoid signaling preference.</li> <li>- <b>Engage a broad ecosystem</b>—including SIs, OEMs, cloud providers, SMEs, and open-source communities—to understand market structure.</li> <li>- <b>Use EME to test feasibility, risk allocation, delivery models, innovation options</b>, and capacity, improving procurement design.</li> <li>- <b>Incorporate validated EME findings into the PPSD, technical specifications and procurement documents.</b></li> </ul>	<ul style="list-style-type: none"> <li>- <b>Don’t skip EME for international procurements.</b></li> <li>- <b>Don’t conduct EME after bidding documents are issued or shortly before bidding</b>, as this may compromise fairness and transparency.</li> <li>- <b>Don’t give any supplier privileged or preferential information</b> or engage in discussions that could create unfair competitive advantage (independent Probity Assurance Advisors can be engaged when relevant and required to oversee the integrity of the process).</li> <li>- <b>Don’t disclose confidential information</b>, budget ceilings, evaluation plans, or draft specifications that could bias the market.</li> <li>- <b>Don’t limit engagement to a small group of incumbent suppliers</b> or create the perception of a preferred supplier</li> <li>- <b>Don’t commit to specific technical specifications</b> or solutions before completing market sounding.</li> <li>- <b>Don’t leave EME undocumented</b>—lack of proper records can raise integrity concerns during audits or Bank reviews.</li> <li>- <b>Don’t use language implying endorsement</b> of a particular vendor, technology, or proprietary standard.</li> <li>- <b>Don’t ignore EME insights</b>—procurement approaches misaligned with market reality risk low competition or failure.</li> </ul>

Table 4.8 summarizes other considerations for market analysis and engagement, including both the high-level market analysis WB teams carry out during early WB operation design and the borrower’s ongoing EME during implementation. Market analysis should be updated for each procurement package through structured and transparent interactions with the private sector—consistent with the World Bank’s EME principles—including open information sessions, written market soundings, and consultations designed to understand market capacity, delivery models, and innovation potential, while avoiding any perception of preference or unfair advantage. These insights must feed back into the PPSD, ensuring that procurement approaches remain realistic, competitive, and aligned with evolving market conditions throughout project implementation.

**Table 4.8: Considerations for market analysis and engagement**

Activity	Considerations
<b>Stakeholder mapping</b>	<ul style="list-style-type: none"> <li>- Identify public, private, and civil society stakeholders critical to the digital DPI ecosystem.</li> <li>- Map roles, incentives, and decision-making influence technology choices.</li> </ul>
<b>Identify legal and institutional framework</b>	<ul style="list-style-type: none"> <li>- Assess enabling legislation, data protection laws, and institutional mandates (governance and beneficiaries) affecting the procurement and deployment of digital systems.</li> <li>- Determine the extent of legal neutrality or potential bias toward certain technologies.</li> </ul>
<b>High-level digital, data, and capacity assessment</b>	<ul style="list-style-type: none"> <li>- Evaluate current digital systems/modules and data infrastructure, including existing systems, interoperability readiness (spanning legislation and policies, legacy systems, datasets, data governance, institutional roles and responsibilities, etc.), and data portability.</li> <li>- Assess the government’s procurement, digital governance, and contract management capacity.</li> <li>- This baseline supports understanding constraints related to digital, data and technology choices, institutional capacities, fit for purpose and value for money, which should all be shared openly with potential vendors during EME to support constructive and honest dialogue that informs procurement approaches.</li> </ul>
<b>High-level analysis of interoperability enablers</b>	<ul style="list-style-type: none"> <li>- <b>Assess the likely scope and any constraints for using recognised open / international standards</b> as key enablers for implementing interoperable systems and data as part of a broader DPI implementation strategy. Conduct a structured scoping of applicable standards (national, international, industry-specific, cloud, security, interoperability, accessibility, open-source, etc.), and provide a clear rationale for why each standard is or is not required for the procurement; this helps avoid over-specification, ensures fit-for-purpose requirements, and supports fair competition across open-source and proprietary solutions.</li> <li>- <b>Assess any specific technical or regulatory requirements</b>, such as interoperability with defined data sources, integration with legacy platforms, compliance with sectoral regulations, adoption of required technical standards, or deployment constraints related to particular cloud environments, as these materially influence design choices and market responses.</li> </ul>
<b>High-level market analysis</b>	<ul style="list-style-type: none"> <li>- <b>Assess a national and international / regional landscape scan of vendors, software and components</b>—open source and proprietary software. Identify market local/regional market presence, procurement flexibility, and deployment approaches (modular/vendor-managed/hybrid, cloud/software-as-a-service, etc.). Analyze security, scalability, functionality, compatibility with existing systems, liability limits, implementation support and maintenance requirements, IP rights, in-house capacities, compatibility with existing systems and modules, exit and transition costs, community strength, alignment with national digital strategy.</li> </ul>

<b>Early engagement with the private sector for innovations</b>	- <b>Organize early consultations / focus groups with solution providers to explore innovations</b> , understand market structure, and surface vendor concerns. Focus on fostering ecosystem-wide alignment.
<b>Public-private partnership (PPP) considerations</b>	- <b>Evaluate whether PPP models are feasible and assess risk of vendor lock-in or data monopolization.</b> PPPs for DPI must include robust exit and transition planning.
<b>Ecosystem capacity scan</b>	- <b>Understand local development capacity, and support ecosystem maturity</b> (e.g., open-source components integration community, language customization and requirements - e.g., right to left languages, integrators, etc.), and skill gaps. This informs which potential open-source software components are accessible on the market, for which component/module of the digital ID/DPI solution, and whether open-source adoption can be sustainable.
<b>PEST and risk analysis</b>	- <b>Conduct a Political Economic Social and Technological (PEST)</b> scan to assess country context and risk appetite related to modular, vendor-managed, or hybrid approaches. Identify risks across 8 PEST framework elements (market, delivery, vendor lock in, cost, capacity, sustainability, pace of change and political context).
<b>Technology Neutrality &amp; Principles-Based Procurement</b>	- Anchor the procurement strategy in international principles such as the 10 Principles on Identification for Sustainable Development <sup>9</sup> , emphasizing neutrality, interoperability, and transparency. Procurement documents should avoid bias toward open-source software or proprietary solutions and focus on functional and performance-based requirements.
<b>Develop procurement strategy</b>	- Define the procurement packages, high-level budget estimates, procurement methods, market approaches, thresholds, and compile the procurement strategy.

<sup>9</sup> See <https://www.idprinciples.org/>

# 5.

## High-level Digital Solution Design and Governance

Strong project governance is essential for integrity and success. Establishing a Technical Review Committee / Task Force (TRC), alongside clearly designated service owners, early in project planning ensures that technical decisions are sound, align with policy and good practices, and take account of procurement and contracting implications. Service owners play a central role in articulating high-level, outcome-based requirements, validating user journeys and ensuring proposed and implemented solutions support long-term sustainability and operational realities. Service owners also play an important role in digital solution implementation, ensuring continuity from conceptualization through delivery.

The TRC—comprising multidisciplinary experts in digital systems, cybersecurity, finance, legal, procurement, data protection, and other relevant domains—provides structured, high-quality technical advisory and evaluation throughout the procurement cycle. This cross-functional expertise supports robust, objective technical and commercial proposal assessments, enabling selection of solutions that best meet project needs, integration requirements, and long-term VfM goals.

Key TRC functions include:

- Providing early technical input to the procurement strategy and planning.
- Ensuring that high-level solution design, specifications, and procurement documents are concise and accessible, and do not discourage participation from competent SMEs and startups.
- Technically reviewing TORs for interoperability, security, and sustainability, and collaborating with the procurement team on how to incorporate these aspects into procurement documents, such as evaluating them in vendor assessments bid.
- Participating in bid evaluations and assisting in explaining the technical information in the bid to non-technical members, while mapping it to the requirements.
- Ensuring alignment with national digital policies and relevant standards.
- Considering sandbox testing or a minimum-viable-product (MVP) approach for high-value or technically complex implementations, including cloud-based DPI or AI solutions.

**In DPI implementations, lock-in risks emerge not only at the software layer but holistically across solution, infrastructure, and security architectures.** Deep reliance on managed, provider-specific services across critical layers—including core platform capabilities and security-critical functions such as identity and access management, logging, monitoring, encryption, and key management—can introduce structural dependencies that are difficult to reverse, even when solutions are technology-neutral. The TRC should assess these multi-layer dependencies during solution design and encourage teams to:

- Identify where dependencies exist at each architectural layer.
- Distinguish between more reversible dependencies and less reversible architectural decisions.
- Document conscious trade-offs when dependencies are introduced.
- Address exit considerations for each layer where significant dependencies exist.

For example, including representatives from e-Government and the cybersecurity agency can promote prioritization of user- and data-driven approaches, “digital by default”, “Once Only” for interoperability, and security and privacy by design.

The TRC requires clear project governance for effective decision making and accountability throughout implementation. TRC members commit to acting within agreed evaluation timelines and prioritizing availability accordingly; this commitment should be formally captured in the TRC’s TOR or governance charter, specifying expected response times, attendance requirements, and escalation procedures for capacity constraints. Governance arrangements should empower the TRC with sufficient authority and operational support to **conduct timely, efficient technical evaluations and decisions, ensuring that procurement and implementation activities are not slowed by avoidable bottlenecks.** At the same time, escalation pathways to senior leadership must be well-defined for issues that exceed the TRC’s mandate. Strong governance is also essential for establishing durable ownership structures on the government side, enabling sustainable operation of DPI solutions by integrating relevant ministries and agencies into the operating model and building long-term operational and maintenance capacities.

The following table outlines key considerations for the high-level design of digital solutions and the development of corresponding technical requirements

**Table 5.1: Considerations for solution requirements design and governance**

Activity	Considerations
Solution charter/concept and vision and strategic alignment	<ul style="list-style-type: none"> <li>- Define the strategic purpose, end-user value and outcomes, and interoperability goals of the digital building block and integrated digital service. Ensure alignment with national digital strategies, e-government framework, and international standards.</li> <li>- Identify legal mandate and institutional ownership (Ministry/Agency that will lead and own the solution).</li> </ul>
Early prototyping and architectural design	<ul style="list-style-type: none"> <li>- Prototypes for iteratively and incrementally testing key components and defining minimum viable product scope, considering users' needs, broader organizational and country contexts, and the outcomes.</li> </ul>
Update market scan and consultations/ early market engagement	<ul style="list-style-type: none"> <li>- <b>Refresh the initial market analysis</b> with early user-driven and human-centric solution high-level blueprints and outcomes. Include evidence from consultations with the vendors to validate the architectural design/scope and propose innovations.</li> <li>- <b>In the design allow flexibility for vendors to propose innovative solution architectures and implementation approaches</b>, including agile and modular implementation options, by incorporating outcome-based requirements and leaving room to recommend alternative technical designs and integration pathways that best meet user needs and project objectives.</li> </ul>
Information security and compliance needs	<ul style="list-style-type: none"> <li>- <b>Specify cybersecurity baseline requirements</b>, including auditability and vulnerability management, security and privacy by design.</li> </ul>

## 6. Bidding Documents and Evaluation

Table 6.1 presents key considerations for finalizing the procurement approach, integrating technical specifications, eligibility and rated criteria, and designing a procurement timeline, along with other specifics of the bidding process. It is important to note that **the technical specification templates included in the Standard Procurement Documents can be fully adapted** by a borrower to reflect specific needs and objectives of the solution or services being procured.

**Table 6.1 is not intended to present a linear “waterfall” flow of activities;** elements should be developed incrementally based on a series of engagements with diverse internal stakeholders and relevant market players. Ultimately, all documentation will need to be complete and approved in readiness for commencing procurement procedures.

**Table 6.1: Considerations for bidding documents and evaluation**

Activity	Considerations
Finalize the procurement approach	<ul style="list-style-type: none"> <li>- <b>Review and finalize the procurement strategy</b>—including whether to use framework agreements, multi-stage RFPs, national or international approaches, or (rarely) direct selection—and determine whether a modular or vendor-manager or hybrid model is appropriate. This review should also assess:               <ul style="list-style-type: none"> <li>o whether software-related procurements fall under Goods (e.g., off-the-shelf, packaged solutions) versus Non-Consulting Services (e.g., cloud services, SaaS, integration, customization, or agile delivery models); when a two-stage RFP is preferable (e.g., when requirements are evolving, when innovation is encouraged, or when bidders may propose alternative technical solutions) versus a one-stage RFP (when design is mature); and when framework agreements can or cannot be applied, weighing trade-offs such as flexibility and speed (framework agreements) versus administrative overhead and market fragmentation.</li> <li>o the strategy must be grounded in project scope, desired outcomes, the updated market scan, and insights from structured market consultations.</li> </ul> </li> </ul>
High-level solution requirements	<ul style="list-style-type: none"> <li>- Clearly articulate needs using <b>vendor- and technology-neutral language</b>, that focuses on standards, key functionalities, outcomes, service levels, and long-term sustainability.</li> <li>- Requirements should remain concise and high-level, as <b>overly lengthy or detailed specifications often signal a lack of clarity and can constrain market innovation</b>.</li> <li>- Where market engagement indicates that both open-source and proprietary solutions are realistic options for the procurement, the requirements should outline the relevant licensing or legal obligations at a high level, without prescribing specific products or technologies, <b>ensuring that functional and outcome-based requirements—not brand names—drive the solution design</b>.</li> </ul>

Develop qualification and evaluation/rated criteria

- **Mandatory qualification criteria** are applied on pass/fail basis. This includes Bidders' relevant experiences, references certifications, JV requirements.
- **Technical and financial qualification requirements should be proportionate and justified, avoiding excessive thresholds** (e.g., overly high annual turnover requirements or unnecessary bid securities) **that may unintentionally exclude capable local or smaller firms**. These requirements should be clearly explained in terms of what they are intended to achieve, the risks of over-specification, and the circumstances in which such conditions do or do not make sense to include, ensuring fair competition and alignment with project outcomes.

**Technical evaluation/rated criteria with weighted ratings**, for example:

- a) **Vendor capabilities and track record**- past experiences, use of local firms, SMEs, universities.
  - b) **Solution design & architecture which includes functional fit** - alignment with business/ high-level requirements, non-functional requirements including scalability- ability to handle peak loads and volumes open standards and interoperability- conformance to standards, and modularity/extensibility- data sharing, capacity to integrate future modules. Require proprietary solution providers to show how they would support data portability. Require bidders to describe how they would support any OSS component (code updates, addressing cybersecurity concerns, patch management, community engagement, product roadmap contributions).
  - c) **Project implementation methodology** which includes implementation approach - agile/ iterative, clarity on roadmap, risk mitigation, proposed software development tools and technologies, use of AI in software customization (how is documented and tested), information/cyber-security requirements.
  - d) **Proposed team** – evaluation should focus on the team's collective capabilities, relevant experience, key proposed staff, and level of effort. **Borrowers should define only the minimum set of required profiles and competencies, allowing vendors to determine the most efficient team composition. Over-prescriptive requirements that mandate large teams or fixed numbers of individuals often inflate costs and exclude efficient delivery models.** Instead of requiring separate specialists for each role, Borrowers should specify competencies rather than headcount, recognizing that in practice a single qualified expert may appropriately cover multiple roles or partial FTE allocations. This approach promotes flexibility, efficiency, and innovation in vendor team design while ensuring that core skills are fully addressed.
  - e) **Capacity building and quality assurance, testing, training plans, and change management**- approach to citizens/businesses service adoption, stakeholder engagement, communications.
  - f) **Handover strategy and sustainability**—evaluation of the vendor's proposed approach to knowledge transfer, documentation, source code access, data migration, and long-term operations and maintenance<sup>10</sup>.
- **Evaluation of Financial Proposals which includes TCO**; Cost components include licenses, hardware assurance, integration with existing systems, implementation costs associated with deploying and customization and configuration, third-party services such as integrators, training, capacity building, project management, and then operating costs which include **recurring costs such as maintenance and support, software updates and upgrades, warranties, help-desk support, and cloud hosting fees**. Require proprietary solution providers to show how they will support data portability.

Procurement timeline, evaluation of proposals

- Define procurement timeline, address bidders' questions, evaluation of technical proposal which **can include demonstrations of proposed solutions** (Note: if demonstration is included as part of the evaluation process, it requires additional consultation with the Bank before the RFP is finalized).

<sup>10</sup> Illustrative weighting ranges for DPI procurements: (a) Vendor capabilities: 10–15%; (b) Solution design and architecture: 25–35%; (c) Implementation methodology: 15–20%; (d) Proposed team: 10–15%; (e) Capacity building and change management: 10–15%; (f) Handover strategy: 10–15%. Teams should also reference the published Library of Rated Criteria for examples, available at <https://www.worldbank.org/en/about/rated-criteria>.

Conditions of Contract

- Borrowers should consciously design clear and simple contracts that enable interoperability, adaptability, collaborative vendor relationships, and outcomes-based delivery. Because much of vendor lock-in occurs through specific contractual terms, Borrowers must pay particular attention to clauses that can restrict government control, flexibility, or access to critical assets—for example, **inappropriate treatment of data as vendor-owned intellectual property**, which can, in the absence of strong data protection laws, lead to governments being locked out of their own citizen data. Key contractual terms that require careful consideration include:
  - a) technology transfer arrangements such as IP ownership, source-code delivery or escrow, and perpetual licenses;
  - b) service level agreements and penalties;
  - c) clear deliverables, acceptance process for the deliverables, KPIs, shared responsibilities across vendors, and interdependencies;
  - d) change management mechanisms;
  - e) post-implementation support;
  - f) warranties;
  - g) financial safeguards such as termination costs;
  - h) milestone payment schedules;
  - i) capped liabilities;
  - j) end-user license agreements, where relevant;
  - k) robust exit strategies, including termination for convenience or cause, change-of-control provisions, transition assistance, data ownership protections, and step-in rights in case of vendor default.

Checklist of recommended DPI-specific contract clauses include:

- a) data ownership—explicit confirmation that all data is owned by the government,
- b) source code access—provisions for code delivery or clear product license and maintenance agreement,
- c) documentation obligations—requirements for comprehensive, continuously updated technical documentation,
- d) interoperability and portability—contractual requirements for compliance with standards and data export in non-proprietary formats, and
- e) right to audit—audit rights.

**(Annex C: Example Contract Clauses for DPI and Integrated Digital Services** includes examples of the above contract clauses that Borrowers and task teams may adopt when preparing contracts for DPI and integrated digital services).

Contract award, complaints procedure

- **Carefully review all assumptions stated in the bidder’s proposal**, including any prerequisites, dependencies, and responsibilities placed on the Purchaser. These assumptions should be tested for realism, alignment with project constraints, and potential risk transfer—ensuring that bidders do not shift undue responsibilities to the government or condition delivery on factors outside their control.
- **Evaluation reports must clearly document how scores were assigned**, how risks and trade-offs were assessed, and how the recommended award decision aligns with the published criteria.
- Review whether the bidder’s proposed terms comply with the government’s data governance, IP, cloud deployment, and cybersecurity requirements—key to avoiding lock-in.
- **Check that the recommended bidder can begin mobilization within the required timeline** and that any pre-conditions (such as access to datasets, environments, or authorizations) are understood.
- **Ensure the PIU provides clear, timely, and well-documented responses to all procurement-related complaints**, ensuring full alignment with World Bank complaints procedures.

## 6.1 Handover strategy

The supplier shall provide a comprehensive and implementable handover strategy, including source code handover (where applicable), detailed data migration and transition plan, and a proposal for multi-year operations and maintenance (O&M) support. All associated costs must be included in the bid and evaluated as part of the financial assessment appropriate to the solution being procured to ensure the solution's long-term sustainability and TCO.

**Table 6.2: Sample Lifecycle Budgeting and Sustainability Model<sup>11</sup>**

Item	Year 1	Year 2	Year 3	Notes
O&M Costs	\$	\$	\$	Routine Administration, monitoring, patching and upgrades
HR Retention (market rates)	\$	\$	\$	Salaries for key staff
Training & Certification	\$	\$	\$	Ongoing capacity building
Data Center Operations	\$	\$	\$	Hosting, backup, DR
Cybersecurity & Compliance	\$	\$	\$	Vulnerability scans, penetration testing, certifications
Software Licensing/ Renewals	\$	\$	\$	Annual or subscriptions based on licenses (if proprietary)
Hardware replacement/ Upgrades	\$	\$	\$	Scheduled replacement or equipment (servers, routers, etc)
Independent Verification & Audits	\$	\$	\$	Annual performance, cybersecurity, and compliance audits
Communications & Support services	\$	\$	\$	Help desk, call center, and public communication costs
Contingency (8% to 10%)	\$	\$	\$	Reserve for unplanned maintenance or upgrade.

## 6.2 References to open-source software in bidding documents

The procurement process should be fair and transparent when comparing open source and proprietary software. Instead of naming specific brands or technologies, it is important to clearly describe what the digital solution needs to fulfill to meet users' needs. Important preferences should be explained. For instance, preference may exist for using certain software—such as input open-source tools, modules, or components in developing the DPI and digital building blocks solutions or integrating digital services. The borrower may have a preference for a certain software or modules already being used or widely adopted, and using these preferences might ease ownership, lower costs, provide more flexibility or strong community support, and be more configurable to fit specific needs.

<sup>11</sup> See Complete Financial Cost Evaluation section of the guidance on Evaluating Bids and Proposals, accessible at <https://thedocs.worldbank.org/en/doc/61a81c4c9c79428afa613f076fa8bb2e-0290032023/original/Evaluating-Bids-and-Proposals-with-Rated-Criteria.pdf> (page 39).

### **Box 6.1: Differentiation between Open-Source Software (OSS) and Commercial Products**

When discussing digital systems, it is important to differentiate OSS and commercial products. OSS refers to software and specifications whose source code is publicly available and can be freely used, modified, and distributed. In contrast, a commercial product typically implies a packaged solution offered by a company, often with proprietary elements, support services, and licensing terms. Borrowers' decisions whether to use open-source or proprietary solutions carries important strategic, technical, financial, and sustainability considerations, all of which should be carefully assessed in the procurement strategy and process.

Further considerations for referring to OSS in high-level solution requirements include:

- Properties of open standards and open source may be part of the requirement specifications, yet these must be framed in a neutral way that does not indicate preference for any specific product, platform, or vendor.
- Specifications should clearly explain how the OSS will work as part of the overall solution being procured and implemented, and how it will operate within, or integrate with, other components of the DPI ecosystem. They should also set expectations for responsible OSS use, including requirements for vendors to contribute back to the main OSS project where appropriate, properly document any changes they make, avoid creating proprietary or undocumented forks, and ensure that modifications remain transparent and portable so as not to introduce new lock-in risks. When mentioning OSS, all language must remain vendor- and product-neutral, ensuring that no specific company, distribution, or implementation is favored and that all qualified vendors and integrators can compete fairly.
- It is not good practice to simply state that software should be open source as this approach lacks clarity on specific objectives, outcomes, and implementation expectations. Instead, requirements should define what aspects of openness are required—such as access to source code, rights to modify and redistribute, and community support—and how these align with the solution's security, operation, sustainability, and security. Instead, OSS properties should be described and justified from the outcome and designed with the DPI solution perspective. A beneficiary government agency can require that:
  - The full code repository—including its complete version history, branches, documentation, and configuration files—shall be owned and exclusively controlled by the beneficiary, ensuring that the agency and any authorized third parties have unrestricted, continuous access for updates, modifications, security reviews, reuse, and further development without dependency on the supplier.
  - Comprehensive and up-to-date technical documentation must be delivered, enabling the beneficiary to fully understand, operate, maintain, modify, and extend the solution independently or through other vendors, thereby safeguarding long-term sustainability and avoiding lock-in.
- Specify the importance of solution flexibility, scalability, and customization, highlighting any advantages in the current context an open-source software module can offer.

- Emphasize the value of security, auditability and transparency, noting that OSS allows for community and third-party code inspections and security audits.
- Require that all solutions, whether open source or proprietary, comply with relevant legal and software licensing requirements, including for any third-party components or libraries.
- Require detailed plans on training and ongoing support, whether OSS provide comprehensive and cost-effective options for building internal expertise or ensuring availability of local or regional expertise for long-term maintenance and operation.
- It is important to note that implementing and operating OSS solutions is not cost-free and requires updating total cost of ownership assessments to reflect implementation and operating costs. There are other important considerations for using and implementing OSS beyond the scope of this procurement guidance.

Annex A: Update on Public Procurement Neutrality for Digital ID Solutions supports this guidance note by helping to preserve procurement neutrality and maintain fair competition. The Annex provides standard, vendor- and technology-neutral wording for key requirements, including documentation and knowledge transfer. In particular, the Annex includes model language such as: *“Comprehensive and up-to-date technical documentation must be delivered...”* to ensure the beneficiary can operate, maintain, modify, and extend the solution independently or through alternative vendors, thereby strengthening sustainability and reducing lock-in risk—without prescribing any specific product, platform, or supplier. Task teams should consult Annex A when reviewing technology-related requirements for bidding documents for Digital ID Solutions to ensure that terminology and framing are consistent with World Bank procurement neutrality standards.

# 7.

## Performance Monitoring and Contract Management

Effective contract management ensures that digital solutions implementation delivers sustained value and accountability. Performance-based payments can be used to independently verify milestones and service outputs, not just deliverables, to incentivize quality.

Contracts must define performance management mechanisms fit-for-purpose and proportionate to what is being procured, so that both the borrower-purchaser and the supplier have a shared, unambiguous understanding of what is expected, by when, and to what standard. For bespoke software or digital solution development, performance is typically managed through well-structured requirements specifications—such as user stories, functional and non-functional requirements, acceptance criteria, deliverables, milestones, and quality gates—rather than “service levels” in the strict sense. In such a scenario, service levels can be specified for post-implementation support. By contrast, Service Level Agreements (SLAs) are most relevant when a supplier provides ongoing “as-a-service” offering (for example, SaaS, cloud hosting, managed services) with measurable operational metrics such as availability, response times, incident resolution, and support desk performance. Hybrid models are common and often appropriate—for example, requirements and acceptance criteria governing the build/customization component, combined with an SLA for support, operations, and maintenance once the solution goes live—ensuring the contract uses the right performance tool for each engagement component.

Implementation can use a sandbox or minimum viable product approach, and a defined “go-live” phase with measurable success criteria and a stabilization period. A well-defined vendor handover strategy—including documentation, data migration, and handover timelines—should be very clear in the contract to ensure continuity post-contract. A robust Contract Management Plan with active risk registers and periodic product/service performance audits maintains oversight and accountability throughout implementation.

**Table 7.1: Considerations for Performance Monitoring and Contract Management**

Activity	Considerations
<b>Contract management</b>	<ul style="list-style-type: none"> <li>- Build incentives for interoperability and openness, such as performance-based payments linked to an integration with other existing systems, and SLA and KPIs with metrics for uptime and API responsiveness.</li> <li>- Ensure the timely review and acceptance of deliverables.</li> <li>- Maintain live risk register and issue logs.</li> </ul>
<b>Training and capacity development</b>	<ul style="list-style-type: none"> <li>- On-line, train the trainer, training sessions for staff and designated administrators.</li> </ul>
<b>Go-live with the minimum viable product</b>	<ul style="list-style-type: none"> <li>- Allocate stabilization period. Prepare user acceptance test (UAT) plan with test cases, load testing, recovery testing, usability and functional testing, cybersecurity testing and user acceptance testing, launching the minimum viable product and performance audits.</li> </ul>
<b>New needs, upgrades, service delivery arrangements</b>	<ul style="list-style-type: none"> <li>- Operational arrangements, including SLAs for the post-implementation support in accordance with severity level classifications and response times, full-time staff equivalents for the support according to support levels, etc.</li> </ul>
<b>Code ownership and exit planning</b>	<ul style="list-style-type: none"> <li>- Source code custody, documentation materials, and access to repositories and databases.</li> <li>- Establish exit strategy and handover protocols to avoid lock-in—even in OSS settings. Ensure clarity on IP ownership.</li> </ul>
<b>Communication and outreach</b>	<ul style="list-style-type: none"> <li>- Stakeholder engagement, launch events, facilitating adoption of digital services through social media, etc.</li> </ul>
<b>Relationship management</b>	<ul style="list-style-type: none"> <li>- Ensuring stakeholders and vendors are aligned and collectively focused on proactively and constructively adapting and responding to change, throughout the lifecycle of contracted service delivery.</li> </ul>

**Table 7.2 Example of performance acceptance criteria and performance-based payments**

Deliverable	Performance Metric	Verification	Linked Payment	Responsible Entity
Identity management system	≥99.5% uptime (excluding pre-agreed maintenance windows)	Automated monitoring reports + system logs + uptime calculation method	20%	PIU + Independent Verification Agent (IVA)
Authentication Response	≤ 3 seconds average response time at agreed load (with defined peak)	Performance/API test results (test scripts, logs, environment specification)	10%	Vendor
Local Capacity Training	≥ 100 staff trained and ≥ X% pass rate on post-training assessment (or competency check)	Attendance records + assessment results + training materials submitted	5%	Vendor, TRC
Stabilization / Hypercare period	90 days live operation with: (i) no Severity-1 incidents attributable to solution; (ii) ≤ X Sev-2 incidents; (iii) agreed defect backlog within thresholds	Incident reports + monitoring logs + post-implementation review report	5%	PIU
Cybersecurity Audit	Compliance with agreed control baseline; critical findings remediated or formally risk-accepted	Pen test & vulnerability scan reports + remediation evidence + retest confirmation	10%	IVA

# 8. Sustainability, Ownership, and Post-Project Continuity

Ensuring sustainability and government ownership after project closure is critical. Before initiating procurements, borrower governments must confirm—better in writing—that O&M and licensing costs will be covered beyond the project’s closure.

To operationalize post-project continuity, borrowers should:

- Identify the permanent institutional owner of the DPI solution—the ministry or organization that will take operational responsibility after the PIU is dissolved—and ensure engagement of this entity immediately at the project design stage.
- Secure a formal written confirmation from the beneficiary government authority that it will allocate operating and maintenance budgets beyond the World Bank operation closing date.
- Develop a phased transition plan that begins no later than 12 months before World Bank operation closing.

Governments should have the option to request source code handover, data migration plans, and multi-year O&M commitments, with all associated costs evaluated during bid assessment for informed decision making.

**Table 8.1: Post-project continuity planning**

Activity	Considerations	Responsibility
Community engagement and contribution planning	- For any implemented OSS components, it is important to ensure community engagement and planning the upgrades.	Vendor, TRC
Monitoring, upgrades, and evaluation	- Provide post-implementation support and maintenance for system stabilization. Define mechanisms for software/system updates (patch management), cybersecurity audits, and continuous SLA checks. This applies equally to OSS and proprietary software integrated in the implemented digital solution.	Vendor, PIU, TRC
Handover of the implemented solution	- Vendors should provide a structured exit strategy and transitional support to maintain solution functionality and institutional capacity beyond the project lifecycle.	Vendor, PIU

# 9.

## Other Considerations

### 9.1 Local market development, SME and start-up participation, and capacity building

Building a strong local digital ecosystem is essential for long-term sustainability of DPI investments. Borrowers should proactively design procurement strategies that encourage the participation of local and regional small and medium-sized enterprises (SMEs) and start-ups, which often drive innovation in the digital sector. To avoid creating barriers to entry, qualification requirements should be proportionate - for example, by accepting relevant project references rather than requiring extensive years of experience, by allowing joint ventures or consortium arrangements that pair local firms with international expertise, and by sizing contract lots to be accessible to smaller firms.

#### Box 9.1: The UK Example of Engaging SMEs

The **UK National Digital Exchange (NDX)**, an AI-enabled digital procurement marketplace launched in 2025, is designed to make it easier for government buyers to access pre-approved cloud and digital services while expanding opportunities for SMEs, with the government projecting a 40 percent increase in SME participation and significant cost savings.

### 9.2 Independent oversight

Borrowers may decide to appoint an Independent Verification Authority (IVA) to strengthen technical oversight and quality assurance during implementation. An IVA can provide continuous, independent monitoring and auditing of deliverables, verify compliance with specifications and cybersecurity requirements, conduct penetration testing and code reviews, and report directly to the PIU. Engaging an IVA helps address technical capacity gaps and ensures that complex solution components are reviewed thoroughly, reducing the likelihood of weak monitoring or low-quality outputs.

## 9.3 Cybersecurity

Cybersecurity performance should be regarded as a core contractual obligation rather than a one-time pre-award requirement<sup>12</sup>. The borrower should specify in the SLA requirements that continuous security assessments are necessary, and add this to evaluations. These assessments should include verification of security patch updates and patch management, vulnerability scans, penetration testing, and incident response drills at specified milestones, such as quarterly or after each major system release. Throughout contract implementation, contractor compliance should be measured against recognized standards. Borrowers should ensure that security requirements are embedded from the outset of solution design and throughout the full development and implementation lifecycle, rather than treated as an afterthought or a one-time pre-award check. Linking payments (output as a Service) to the compliance level can help achieve the desired security level.

---

<sup>12</sup> Relevant cybersecurity provisions hardwired into the World Bank's published Standard Procurement Documents (SPDs). These provisions provide a baseline framework for managing cybersecurity risks and should be the starting point for any digital procurement with a cybersecurity risk exposure.

# 10.

## Conclusion

Digital procurement is not just about acquiring technology—it is about organizational culture and behavioral change, building capability, trust, and sustainable institutions and digital ecosystems. By aligning project needs with available market capacity, ensuring cybersecurity, and planning for sustainability, TTLs and borrower teams can future-proof investments and contribute to inclusive, resilient digital transformation.

This technical guidance note on procurement of DPI and Services under World Bank operations does not address all aspects of DPI implementation, such as broader institutional, legal, and policy frameworks. The authors of this note acknowledge that areas extending beyond the scope of this work (including potential development of new Standard Procurement Documents applying a modular approach tailored to cloud, XaaS, and digital subscription services) represent important next steps requiring further work by World Bank Procurement and Digital communities.

# 11. Annexes

## **11.1 Annex A: Update on Public Procurement Neutrality for Digital ID Solutions**

Annex A provides standard, vendor- and technology-neutral definitions of open-source software, proprietary software, open standards, and open data, as well as guidance on procurement neutrality in the context of digital identity systems. It supports Section 6.2 and the technology-neutral procurement guidance throughout this document.

## **11.2 Annex B: Digital Service Delivery Procurement Principles and Framework Agreement Templates**

Annex B provides a practical template for framework agreements in the DPI and digital services context, including Digital Service Delivery Principles, lot structures, and a detailed call-off process. It supports the framework agreement guidance in the dedicated subsection and provides actionable examples for Borrowers.

## **11.3 Annex C: Example Contract Clauses for DPI and Integrated Digital Services**

Annex C provides example contract clauses that Borrowers and task teams may adapt when preparing contracts for the procurement of Digital Public Infrastructure (DPI) and integrated digital services under World Bank-financed projects. The clauses address five critical areas that are essential to ensuring government ownership, long-term sustainability, interoperability, and accountability in DPI procurement.

## Annex A: Update on Public Procurement Neutrality for Digital ID Solutions

This document accompanies the ‘Technical Procurement Guidance for Digital Public Infrastructure (DPI) and Services’. It provides standard, vendor- and technology-neutral definitions of open-source software, proprietary software, open standards, and open data, as well as guidance on procurement neutrality in the context of digital identity systems.

1. It is important to clearly distinguish the following concepts:
  - **Open-Source Software (OSS):** Software whose source code is accessible to everyone, which can be studied, modified, or distributed freely. However, not all open-source software meets the criteria of a Digital Public Good (according to the classification of the Digital Public Good Alliance).
  - **Proprietary Software:** Generally, it requires a paid license to be used (one-time or recurring payment), with non-accessible source code. Also known as “closed” or commercial software. Not all proprietary software causes vendor lock-in; it depends on data portability, interoperability, customization possibilities, licenses, and support.
  - **Open Standards:** Publicly available and developed through a collaborative process implementable by multiple suppliers. Used by both OSS and proprietary software, but open source software using proprietary standards cannot be freely distributed. A solution using a closed standard can surpass an open standard if it is widely adopted (e.g., ISO standards).
  - **Open Data:** Open data is publicly accessible data that anyone can use, reuse, and share freely. It is usually provided with a license that allows free and unrestricted access, promoting transparency, collaboration, and innovation.
2. Historically, public procurement for identity systems was structured as large turnkey contracts, which limited competition and innovation. To address these challenges, two major initiatives have emerged as solutions for digital identity systems: **MOSIP** and **OSIA**:
  - **MOSIP** is an OSS designed for foundational identity systems, offering essential components such as the registration client (an interface for capturing biographic and biometric data) and the backend database that stores all registered individuals. Typically when countries adopt MOSIP for these core modules, major industry providers continue to be awarded contracts for additional components, such as Automated Biometric Identification Systems (ABIS), biometric enrollment devices, or identity cards. This approach also creates new opportunities for system integrators (IS). MOSIP is based on open standards, and it is possible to build “adapters” that perform the translation from one standard to another (to make MOSIP compatible with OSIA standards). Many vendors, for example in the identity ecosystem providing the ABIS component for biometric deduplication, have shown compliance with both MOSIP and OSIA standards.
  - **OSIA** contributed to developing standard interfaces as an open standard to ensure interoperability between different modules of identity management systems. This approach is now reflected in ITU-T Recommendation<sup>13</sup> X.1281 (03/2024) which is technically equivalent

---

<sup>13</sup> See <https://www.itu.int/rec/T-REC-X.1281-202403-I>

to OSIA and specifies standardized APIs to connect identity system building blocks. By creating a level playing field, OSIA/ITU-T X.1281 allows solutions from various vendors to be compatible with each other, fostering competition and encouraging innovation.

3. **The ID4D initiative adopts a neutral stance on technology and does not preferentially support any specific technology, such as MOSIP.** The choice of open source software components or other technological solutions is up to the countries. The World Bank Group helps countries assess their needs and options while ensuring neutrality in all technological engagements. The actions of the ID4D initiative are guided by the 10 Principles on Identification, which recognize the importance of open standards and technology neutrality: [10 Principles on Identification](#).

- **Neutrality does not mean “no requirements.”** It means avoiding brand/product mandates while requiring interoperability outcomes—for example, by specifying compliance with recognized open standards for interfaces/APIs (e.g., ITU-T X.1281, Open ID Connect, etc.) so modules can be replaced and integrated without lock-in.
- **The World Bank Group promotes open standards and specifications by collaborating with global standardization bodies and Digital Public Goods (DPGs), such as GovStack, OSIA, and the OpenID Foundation.** While the ID4D initiative raises awareness about open standards and open source software components, the World Bank Group teams only provides technical assistance at the request of the government, regardless of the selection of technology solution by governments.
- **Countries that choose MOSIP and a modular approach (splitting the market between different components of the identity system) generally call upon a system integrator.** A system integrator acts as a coordinator, ensuring seamless integration of all elements of a country’s identity system, including any open source software components. It is acceptable for countries to specify in terms of reference (TOR) in the background of the current situation for the system integrator the types of internal systems or components used, such as the registration client software or the source of existing enrollment kits. That does not limit competition among companies providing integration services, and technology providers can still participate in tenders.

## Annex B: Digital Service Delivery Procurement Principles and Framework Agreement Templates

This document accompanies the 'Technical Procurement Guidance for Digital Public Infrastructure (DPI) and Services' as a reference example for Borrowers to tailor to their local needs. This document comprises two interrelated sections:

- A suggested **high-level call for framework agreement applications** (primary procurement); and
- A suggested **high-level call-off process** from this framework agreement, once it's awarded (secondary procurement).

This is provided as an example, and it needs to be assessed by Borrowers depending on their project needs and explained in their Project Procurement Strategy for Development (PPSD).

## Suggested high-level call for framework agreement applications

### Framework agreement title:

Digital Delivery Services 1

### Type of framework agreement:

Services

### Short description:

Borrower as the contracting authority intends to put in place a pan government collaborative framework agreement for use by [country] public sector buyers. These bodies need a compliant procurement route to access digital delivery services as either whole teams or individual digital specialists.

This framework agreement is a closed panel, and its constitution won't change during the term of the framework agreement (other than vendors being removed from the panel; no additional or replacement vendors may be added).

Vendors supplying services through this framework agreement must work according to the World Bank's *Digital Service Delivery Principles and associated Guidance Note* [[link](#)], which is summarized as follows:

1. Understand and meet users' needs through service design;
2. Ensure inclusive and equitable access;
3. Be open by default;
4. Build trust by being secure and respecting privacy by design;
5. Understand the ICT and digital supply ecosystem;
6. Procure sustainably and for resilience;
7. Integrate and adapt;
8. Consider cloud first;
9. Configure, rather than customize; and
10. Measure what matters

Vendors are not guaranteed being awarded any call-off contracts under this framework agreement, and the Borrower makes no commitments on possible volumes of services. This framework agreement is non-exclusive, and the Borrower reserves the right to procure the same or similar services from vendors outside of this framework agreement.

The Borrower, without prejudice to any other remedy for breach of the framework agreement or call-off contract, may terminate this framework agreement immediately, by notice in writing if the vendor:

- In the judgement of the Borrower, has engaged in fraud and / or corruption; or
- During the term of the framework agreement, ceases to be qualified or eligible; or
- Purports to assign, or otherwise transfer or dispose of this framework agreement and / or call-off contract, in whole or in part, without the prior written consent of the Borrower or the buyer; or
- Becomes bankrupt or otherwise insolvent; or
- Consistently fails to comply with the Digital Service Delivery Principles; or
- Consistently does not submit proposals for call-off contracts, when requested by buyers, or consistently fails to submit a technically qualified proposal; or
- Fails to perform any other obligation under the framework agreement and / or any awarded call-off contract.

### **Buyers:**

The following public sector bodies (and any future successors to these organizations) are permitted to procure services under this framework agreement:

[TBC - informed by country-specific projects pipeline]

### **Estimated total value:**

[TBC - informed by country-specific projects pipeline and market engagement]

### **Information about lots:**

This framework agreement is divided into lots: Yes [subject to market analysis and the PPSD]

Tenders may be submitted for one or all lots

Maximum number of lots that may be awarded to one tenderer: 2

### **Secondary procurement methods:**

The secondary procurement methods that apply to the selection of a vendor for the award of a call-off contract under this framework agreement are:

- Competitive proposals through mini competitions; and
- Direct selection based on a buyer's objective criteria grounded on previous experience.

### **Lot 1: Teams of Digital Specialists**

Lot 1 description: Vendors of teams of digital specialists can help [country] to research, test, design, build, release, iterate, support, retire or govern (depending on the capabilities specifically required for) a digital service, by applying user-centered and agile delivery methodologies.

An example of a project involving a team of specialists includes:

“A multidisciplinary agile delivery team to develop a new cloud-based digital service for civil registrations, including implementing a Data Exchange System for interoperability with other government services. The current civil registrations service is paper-based and manual, and the [country] team is at the beginning of their digital transformation journey, so upskilling, capacity building and practical coaching will be expected from the team of specialists throughout contracted service delivery”.

Vendors applying for Lot 1 teams of digital specialists must provide at least one of the following listed digital specialist capabilities, and at least one of the following corresponding individual digital specialists roles:

[This is a suggested list based on general experience; this can differ based on project needs and should be reflected in the PPSD]

Lot 1: Teams of Digital Specialist Capabilities	Individual Digital Specialists Roles
Architecture	<ul style="list-style-type: none"> <li>Business Architect</li> <li>Data Architect</li> <li>Enterprise Architect</li> <li>Network Architect</li> <li>Security Architect</li> <li>Solution Architect</li> <li>Technical Architect</li> </ul>
Data	<ul style="list-style-type: none"> <li>Analytics Engineer</li> <li>Data Analyst</li> <li>Data Engineer</li> <li>Data Ethicist</li> <li>Data Governance Manager</li> <li>Data Scientist</li> <li>Digital Evaluator</li> <li>Machine Learning Engineer</li> <li>Performance Analyst</li> </ul>
Product	<ul style="list-style-type: none"> <li>Business Analyst</li> <li>Product Manager</li> <li>Service Owner</li> </ul>
Agile Delivery	<ul style="list-style-type: none"> <li>Program Delivery Manager</li> <li>Digital Portfolio Manager</li> <li>Delivery Manager</li> </ul>

Quality Assurance Testing (QAT)	QAT Analyst Test Engineer Test Manager
Software Development	Development, Security and Operations (DevSecOps) Engineer Frontend Developer Software Developer
User-Centered Design	Accessibility Specialist Content Designer Content Strategist Graphic Designer Interaction Designer Service Designer Technical Writer User Researcher
ICT Operations	Application Operations Engineer Business Relationship Manager Change and Release Manager Command and Control Centre Manager End User Computing Engineer Incident Manager Infrastructure Engineer Infrastructure Operations Engineer ICT Service Manager Problem Manager Service Desk Manager Service Transition Manager
Governance	Financial Operations (FinOps) Specialist Commercial and Procurement Specialist Audit and Risk Specialist

Lot 1 award criteria:

Quality Weighting: 100%

Price Weighting: 0%

Lot 1 pricing:

Vendors applying for Lot 1 teams of digital specialists must provide maximum day rates for at least one of the individual digital specialist roles corresponding to the digital specialist capability or capabilities for which they're applying.

Vendors awarded a place on Lot 1 of this framework agreement will have their pricing evaluated by buyers during their mini competitions.

Minimum number of vendors for Lot 1: [TBC - informed by country-specific projects pipeline and market engagement]

Maximum number of vendors for Lot 1: [TBC - informed by country-specific projects pipeline and market engagement]

Lot 1 estimated value:

[TBC - informed by country-specific projects pipeline and market engagement]

Duration of the framework agreement in months:

[Maximum period of three (3) years]

This framework agreement is subject to renewal:

[Option to extend by up to a further two (2) years, if the initial engagement has been satisfactory]

## **Lot 2: Individual Digital Specialists**

Lot 2 description: Vendors of individual digital specialists can help [country] to contribute to either researching, testing, designing, building, releasing, iterating, supporting, retiring or governing (depending on the specialist capabilities specifically required for) a digital service, by applying user-centered and agile delivery methodologies.

An example of a project involving individual digital specialists includes:

“A Service Designer to join an existing multidisciplinary agile delivery team that’s developing a new cloud-based digital service for civil registrations, which includes implementing a Data Exchange System for interoperability with other government services. The current civil registrations service is paper-based and manual, and the [country] team is at the beginning of their digital transformation journey, so upskilling, capacity building and practical coaching will be expected from the specialist throughout contracted service delivery”.

Vendors applying for Lot 2 individual digital specialists must provide at least one of the following listed roles corresponding to the required specialist capabilities:

[This is a suggested list that can differ based on project needs and should be reflected in the PPSD]

Digital Capabilities	Lot 2: Individual Digital Specialists Roles
Architecture	Business Architect Data Architect Enterprise Architect Network Architect Security Architect Solution Architect Technical Architect
Data	Analytics Engineer Data Analyst Data Engineer Data Ethicist Data Governance Manager Data Scientist Digital Evaluator Machine Learning Engineer Performance Analyst
Product	Business Analyst Product Manager Service Owner
Agile Delivery	Program Delivery Manager Digital Portfolio Manager Delivery Manager
Quality Assurance Testing (QAT)	QAT Analyst Test Engineer Test Manager
Software Development	Development, Security and Operations (DevSecOps) Engineer Frontend Developer Software Developer

User-Centered Design	<ul style="list-style-type: none"> <li>Accessibility Specialist</li> <li>Content Designer</li> <li>Content Strategist</li> <li>Graphic Designer</li> <li>Interaction Designer</li> <li>Service Designer</li> <li>Technical Writer</li> <li>User Researcher</li> </ul>
ICT Operations	<ul style="list-style-type: none"> <li>Application Operations Engineer</li> <li>Business Relationship Manager</li> <li>Change and Release Manager</li> <li>Command and Control Centre Manager</li> <li>End User Computing Engineer</li> <li>Incident Manager</li> <li>Infrastructure Engineer</li> <li>Infrastructure Operations Engineer</li> <li>ICT Service Manager</li> <li>Problem Manager</li> <li>Service Desk Manager</li> <li>Service Transition Manager</li> </ul>
Governance	<ul style="list-style-type: none"> <li>Financial Operations (FinOps) Specialist</li> <li>Commercial and Procurement Specialist</li> <li>Audit and Risk Specialist</li> </ul>

Lot 2 award criteria:

Quality Weighting: 100%

Price Weighting: 0%

Lot 2 pricing:

Vendors applying for Lot 2 individual digital specialists must provide maximum day rates for at least one of the individual digital specialist roles listed.

Vendors awarded a place on Lot 2 of this framework agreement will have their pricing evaluated by buyers during their mini competitions.

Minimum number of vendors for Lot 2: [TBC - informed by country-specific projects pipeline and market engagement]

Maximum number of vendors for Lot 2: [TBC - informed by country-specific projects pipeline and market engagement]

Lot 2 estimated value:

[TBC - informed by country-specific projects pipeline and market engagement]

Duration of the framework agreement in months:

[Maximum period of three (3) years]

This framework agreement is subject to renewal:

[Option to extend by up to a further two (2) years, if the initial engagement has been satisfactory]

## Suggested high-level call-off process

[Subject to market analysis and the PPSD, it's anticipated that this framework agreement could include at least two service lots, which should both be relevant and of interest to small and medium-sized enterprises (SMEs) and large vendors, domestically and internationally:

- **Lot 1: teams of specialists** - for example, “a multidisciplinary agile delivery team to develop a new cloud-based digital service for civil registrations, including implementing a Data Exchange System for interoperability with other government services”; and
- **Lot 2: individual specialists** - for example, “a Service Designer to join an existing multidisciplinary agile delivery team that’s developing a new cloud-based digital service for civil registrations, which includes implementing a Data Exchange System for interoperability with other government services”.

Vendors awarded call-off contracts for either Lot 1 or Lot 2 must support buyers to align with the Digital Service Delivery Principles.

This suggested high-level call-off process assumes the above framework agreement design.]

## Defining requirements

Borrowers should develop concise and plain language Terms of Reference (TORs), which include descriptions of:

- **Problems** they’re trying to solve in collaboration with their country counterparts;
- **Outcomes** and **impact** they want to achieve;
- Who the **users** are **and their needs** that will need to be met;
- **Current situation** and why the work is required;
- Any relevant **work that’s already been done**;
- Who the **existing team** is that the vendor will be working with;
- **Latest date** for contracted services to start;
- Expected **contract length**, including any extension options; and
- **Budget available** for the work (either as a maximum daily rate for individual specialists, or to cover the total project including extension options for teams of specialists).

## High-level flow

See [Appendix 1](#) for a detailed call-off process based on the following high-level flow:

1. **Engage early** with framework vendors;
2. **Finalize** specification, assessment criteria and draft call-off contract;
3. **Publish** the opportunity on [portal / widely circulated medium used by Borrowers];

4. **Respond** to vendors' questions;
5. **Evaluate** via mini competition:
  - a. Stage 1: conduct shortlisting;
  - b. Stage 2: conduct further assessments;
6. **Award** and publish your decision on [portal / widely circulated medium used by Borrowers]; and
7. **Complete** your call-off contract.

## Mini competitions

Borrower will engage framework agreement vendors as required, through call-off contracts. Depending on the likely number of vendors that would be available through this framework agreement - to be established during early market engagement (EME) - it's anticipated that **a two-stage competition** will be followed to appoint a vendor to provide either **a team of at least two specialists or an individual specialist** (e.g. a Software Engineer, a Service Designer, a User Researcher, an Agile Delivery Manager, etc.).

## Direct selection

The buyer negotiates either a lumpsum or time-based contract (depending on the assignment) with a vendor who already has a framework agreement. The negotiations are based on the TOR for the specific call-off contract.

Technical negotiations may cover:

- Whether the vendor's proposed approach, work plan, and team structure properly meet the TOR requirements;
- Confirming that the digital specialist roles included in the framework agreement (and evaluated during the primary procurement) are part of the team; and
- Reviewing the qualifications and suitability of any replacement or additional digital specialist roles who were not evaluated during the primary procurement.

Financial negotiations may cover confirming that:

- Expert rates (or, for lumpsum contracts, the rates used to calculate the contract ceiling) do not exceed the rates agreed in the framework agreement, except for any allowed price adjustments;
- Reimbursable expenses (or, for lumpsum contracts, the rates used to calculate the ceiling amount) do not exceed what was agreed in the framework agreement, subject to permitted adjustments. These amounts are also used to calculate taxes and payments for any additional services requested by the buyer;
- The vendor's tax obligations in [country] are clearly defined in the contract. This includes specifying which taxes the vendor pays directly and which taxes the buyer withholds and pays on the vendor's behalf, such as:

- Local indirect taxes (e.g., sales tax, excise tax, VAT) applied to invoices; and
- Any additional local indirect taxes on fees paid to non-resident experts working in [country].

In both cases of mini competitions or direct selection, vendors will provide outcome-based services under clearly defined pieces of work - 'statements of work' (SoWs).

## Pricing

During stage 2 further assessments of the two-stage mini competition process, vendors will be required to submit a pricing proposal. For mini competitions for teams of specialists, vendors will be asked to provide a detailed breakdown of their total solution price, identifying the individual specialist roles and their costs, as well as any additional pricing for products or services to be used (e.g. hosting infrastructure for prototyping environments).

During the compliance and evaluation phase of stage 2 further assessments, you should check that the specialist day rates quoted do not exceed the maximum day rates agreed with vendors (as per their framework agreement prices).

Fees, charge rates or pricing mechanisms, and any other associated costs, will be agreed with each vendor and will be valid for the term of the framework agreement.

## Appendix 1: Suggested detailed call-off process

1. **Engage with framework vendors** - conduct at least one round of pre-procurement EME to share draft requirements and draft evaluation approach, together with any supporting documentation such as your draft business case and draft call-off contract, including the initial SoW.

Conducting more than one round of EME provides an opportunity to demonstrate how vendors' feedback has helped objectively and incrementally shape your approach to market. This also helps to minimize the number of questions asked by vendors once the procurement formally starts.

If you have a very limited understanding of your requirements, a basic concept or idea, you can choose to run bilateral EME sessions with a subset of framework vendors. For fairness and transparency, the list of invitees to bilateral EME sessions should be a representative sample. If your requirements are more developed, or you want to make the market aware of your forthcoming procurement activity, you should use the complete list of framework vendors. Remember to keep thorough records of all EME activities;

2. **Finalize specification, assessment criteria and draft call-off contract** - finalize your outcomes-based requirements and evaluation approach (including evaluation timescales), the draft call-off contract and initial SoW.

As part of the evaluation approach, you'll need to specify how you'll score vendors. You can choose to use the default scoring criteria of 0 to 3 or define your own (up to 10 levels). The default scoring system is below:

- 0 - Not met or no evidence;
- 1 - Partially met;

- 2 - Met; and
- 3 - Exceeded

You should score each criterion individually, without using half-scores. You should exclude vendors who get less than 'Met' for any essential skills and experience criteria.

- Demonstrate extensive expertise in modern, cloud technologies and their application in a large business environment;
- Demonstrate substantial cyber security expertise and leadership;
- Demonstrate a track record of user-centered design and agile approaches to delivery;
- Demonstrate a track record of mentoring junior engineers and other teams to become self-sufficient;
- Experience of solution architecture within a broader organizational framework to implement security by design principles, achieve resilience and delivery value for money;
- Experience of developing digital services "in the open", using tools such as GitHub; and
- Demonstrate an understanding of and experience aligning ways of working to, the World Bank's Digital Service Delivery Principles and associated Guidance Note [[link](#)].

#### ***Examples of essential skills and experience criteria***

State in your requirements how many vendors will be shortlisted for stage 2 further assessments. The scoring criteria you define will be applicable for both stage 1 shortlisting and stage 2 further assessments.

3. **Publish the opportunity on [portal / widely circulated medium used by Borrowers]** - all documentation should be made available to all vendors to ensure fairness, transparency, equal treatment and non-discrimination;
4. **Respond to vendors' questions** - address all queries raised by vendors within the stated timescales, which may include making non-material updates to the information published (i.e. outcomes-based requirements, evaluation approach, draft call-off contract and draft SoW);
5. **Evaluate via mini competition:**
  - a. **Stage 1: Shortlisting** - all vendors who wish to be considered for stage 1 shortlisting must provide a response to your essential and nice-to-have requirement questions. Vendors who don't meet one or more of your essential criteria can be excluded from the procurement.

Vendors need to provide individual responses against each shortlisting question, and each response should not exceed 300 words. You have the discretion to exclude any vendor who exceeds this limit, or to evaluate only the first 300 words of their response. You must treat all vendors fairly and equally.

It's recommended that a minimum of 3 people with domain / sector specific expertise (e.g. cyber security specialists, urban mobility specialists, etc) evaluate vendors' responses. Ensure that you maintain a fully documented audit trail of the results and final moderated shortlisting scores, which will be useful when providing feedback to the participating vendors.

At the shortlisting stage you enter the total score (not the weighted score) for each vendor who has responded. Weightings are only used in the calculation of the final overall score for each vendor at the end of stage 2: Further assessments.

When defining your requirements, you need to state how many vendors you want to take through to stage 2 further assessments (a minimum of 3). The number you entered should be used to generate your shortlist. It's acceptable if the number of vendor responses is fewer than expected. If only 1 vendor responded then you have discretion to take this single vendor forward to further assessment, or to cancel your procurement and start again.

You can shortlist the vendors who:

- Meet all the essential skills and experience;
- Can start work when you need them to;
- Can work within your daily rate budget (specialist vendors only);
- Provide the most nice-to-have skills and experience; and
- Provide the highest-scoring evidence of their skills and experience.

If there are tied scores or very close scores, you have the discretion to take more vendors forward than you originally stated.

You must inform vendors if they have not been shortlisted and explain why they didn't meet the requirements. You're not obliged to provide detailed feedback at the shortlisting stage, but you should provide this once all evaluation steps have been completed.

- b. **Stage 2: further assessments** - issue further assessment documents, review proposals and evaluate vendors.

The further assessment stage may include, but is not limited to:

- Providing work histories or supporting statements [maximum word count / page numbers TBC];
- Providing written proposals [maximum word count / page numbers TBC];
- Providing case studies or evidence of previous work [maximum word count / page numbers TBC];
- Presentations [maximum slide numbers / duration TBC];
- Scenarios or tests [maximum word count / page numbers / durations TBC];
- Interviews [maximum duration TBC];
- Providing references [maximum word count / page numbers TBC]; etc.

Each further assessment method should be limited in size or duration by a maximum number of either word count or page numbers, length of presentations, scenarios or tests, and interviews, which are realistic and proportionate to the nature and complexity of each assessment method.

6. **Award and publish your decision on [portal / widely circulated medium used by Borrowers]**  
- notify your vendors, and publish your contract award decision;
7. **Complete your call-off contract** - put together and countersign your contract, including the initial SoW.

## Annex C: Example Contract Clauses for DPI Procurement

### Introduction and Purpose

The clauses in this Annex of the “Technical Procurement Guidance for Digital Public Infrastructure (DPI) and Services” represent examples intended to illustrate the types of provisions that should be included in contracts for DPI and integrated digital services procurement. They are not mandatory templates and should be adapted by task teams and Borrowers to reflect:

- **The specific DPI domain** (digital identity, payments, data exchange, integrated digital services) and the applicable technical standards for that domain;
- **The delivery model** selected in the PPSD (modular, vendor-managed, or hybrid), which affects the balance between government and vendor responsibilities;
- **The Borrower’s institutional capacity** and legal framework, including existing data protection legislation, procurement regulations, and IT governance arrangements;
- **The contract type** (single contract, framework agreement with call-offs, or multi-lot structure as described in the main guidance and Annex B); and
- **The software approach** (COTS-based, custom development, open-source, or hybrid), which particularly affects source code and licensing provisions

Task teams are encouraged to consult with procurement specialists and legal counsel when adapting these clauses, and to review them alongside the main body of the Guidance, Annex A (Procurement Neutrality), and Annex B (Framework Agreement Templates) to ensure consistency across the procurement package.

**The five areas covered are:** (l) Data Ownership; (m) Source Code Access; (n) Documentation Obligations; (o) Interoperability and Portability; and (p) Right to Audit. Each section includes a rationale explaining why the clause matters for DPI procurement, example contract language, and a drafting note with practical guidance.

### (l) Data Ownership

**Rationale:** In DPI contexts, data—including individual identity records, transaction logs, registry entries, and administrative data—is a sovereign asset. Without explicit contractual provisions, there is a risk that the Contractor may claim rights over data generated through the system, particularly where proprietary analytics, data structures, or enrichment processes are applied. This example clause ensures unambiguous government ownership of all data from the outset, consistent with the World Bank’s emphasis on country ownership and sustainability.

### Example Contract Clauses:

All data—including but not limited to citizen and beneficiary records, transaction data, registry entries, metadata, system logs, configuration data, analytics outputs, and any data generated, collected, processed, stored, or derived through or in connection with the System—shall be and remain the sole and exclusive property of the Purchaser. The Contractor shall have no right, title, or interest in any such data.

The Contractor shall not use, copy, disclose, sell, license, transfer, or otherwise make available

any Purchaser data for any purpose other than the performance of its obligations under this Contract, without the prior written consent of the Purchaser.

Upon expiration or termination of this Contract, or at any time upon the Purchaser's request, the Contractor shall deliver to the Purchaser a complete and current copy of all Purchaser data in a format and on media specified by the Purchaser, together with all encryption keys, passwords, and access credentials necessary to access and use such data. Following confirmation of successful data transfer, the Contractor shall securely delete all copies of Purchaser data in its possession or control, including any backups, and shall provide written certification of such deletion.

The Contractor shall implement and maintain appropriate technical and organizational measures to protect Purchaser data against unauthorized access, loss, destruction, or alteration, in accordance with applicable data protection laws and the data protection requirements specified in the Terms of Reference.

The data ownership provisions of this Article shall survive the expiration or termination of this Contract.

**Drafting Note:** Borrower and Task teams should adapt this clause to the specific data categories relevant to the DPI system being procured (e.g., biometric data for digital identity, financial transaction records for payments infrastructure). Where the Borrower's legal framework includes data protection legislation (e.g., GDPR-equivalent laws), the Terms of Reference should cross-reference those requirements. For systems processing personally identifiable information (PII), consider adding specific provisions on data localization, cross-border transfer restrictions, and breach notification obligations.

## **(II) Source Code Access**

**Rationale:** Access to source code is another key measure to avoiding vendor lock-in in DPI and integrated digital services procurements. Without source code access, the government cannot maintain, modify, or extend the system independently or through alternative vendors after the contract ends. It distinguishes between Custom Software (where full ownership transfers) and COTS/third-party software (where license rights are secured).

### **Example Contract Clauses:**

**Custom Software.** All Intellectual Property Rights in Custom Software developed under this Contract shall vest in the Purchaser upon creation. The Contractor shall deliver to the Purchaser the complete source code of all Custom Software, including all source files, build scripts, configuration files, database schemas and migration scripts, API specifications, test suites, and related documentation, in a form that enables the Purchaser or any authorized third party to compile, deploy, maintain, modify, and extend the software without dependency on the Contractor.

**COTS and Third-Party Software.** For any Commercial Off-the-Shelf (COTS) software or third-party software components incorporated into the System, the Contractor shall grant or procure for the Purchaser an irrevocable, perpetual, royalty-free, non-exclusive, transferable license to use, copy, modify (including through third-party service providers), and sublicense such software for the purpose of operating, maintaining, and extending the System. The license shall not be contingent on the continuation of any relationship between the Purchaser and the

Contractor or any third party.

Where the Contractor is unable or unwilling to deliver source code for COTS or third-party components, the Purchaser may request establishing the Source Code Escrow.

**Source Code Escrow.** The Contractor shall, at its own cost, establish and maintain a source code escrow arrangement with a reputable independent escrow agent approved by the Purchaser. The escrow shall cover the complete source code, build environment specifications, and all documentation necessary to compile and deploy the software. Release conditions shall include: (a) the Contractor's insolvency, bankruptcy, or cessation of business; (b) the Contractor's material breach of this Contract that is not cured within the specified cure period; (c) the Contractor's failure to provide contracted maintenance and support services; or (d) the expiration or termination of this Contract.

The Contractor shall ensure that all source code delivered or held in escrow is accompanied by: (a) a description of the development environment, including compilers, interpreters, libraries, frameworks, and tools required to build and deploy the software; (b) build and deployment instructions sufficient for a competent third party to reproduce the production environment; and (c) a complete version history.

The Contractor shall update the source code delivery or escrow deposit no less frequently than with each major release, and in any event within thirty (30) days of any material modification to the software.

**Drafting Note:** The distinction between Custom Software and COTS is critical. For DPI systems built on open-source software (e.g., MOSIP for digital identity), the source code is publicly available, but the clause should still address any customizations, configurations, or extensions developed by the Contractor. The escrow provision is a fallback for situations where full source code delivery is not commercially feasible for proprietary components. Task teams should consult Annex A for guidance on framing OSS and proprietary software provisions in a technology-neutral manner.

### **(III) Documentation Obligations**

**Rationale:** Comprehensive technical documentation is a prerequisite for the government's ability to operate, maintain, and evolve DPI systems independently. Without continuous documentation, the government risks becoming dependent on the original Contractor for even routine maintenance tasks. This clause establishes documentation as a contract deliverable with specific quality and update requirements.

#### **Example Contract Clauses:**

The Contractor shall prepare and deliver comprehensive technical documentation for the System, including but not limited to: (a) system architecture documentation, including component diagrams, data flow diagrams, and integration architecture; (b) detailed design documentation for all modules and subsystems; (c) database schemas, data dictionaries, and entity-relationship diagrams; (d) API specifications and interface documentation in machine-readable formats (e.g., OpenAPI); (e) source code documentation, including inline comments and code-level documentation; (f) deployment and operations manuals, including installation procedures, configuration guides, and environment specifications; (g) system administration and maintenance manuals; (h) user manuals and training materials; (i) security documentation,

including threat models, security architecture, and incident response procedures; and (j) test documentation, including test plans, test cases, and test results.

Documentation shall be treated as a formal Deliverable and shall be subject to acceptance by the Purchaser in accordance with the acceptance procedures specified in this Contract. Documentation that is incomplete, inaccurate, or not current shall not be accepted.

The Contractor shall maintain all documentation in a current state throughout the Contract Term. Documentation shall be updated within fifteen (15) business days of any material change to the System, including design changes, configuration changes, new releases, patches, and modifications. The Contractor shall maintain a documentation change log identifying all updates, the date of each update, and the changes made.

All documentation shall be delivered in editable, non-proprietary formats (e.g., HTML, wikis, or editable word processing formats) and organized in a version-controlled repository accessible to the Purchaser. The Contractor shall not deliver documentation solely in proprietary formats that require licensed software to view or edit.

The documentation obligations of this Article shall apply equally to all subcontractors and shall be incorporated into all subcontracts. The Contractor shall be responsible for ensuring that subcontractor documentation meets the same standards as its own.

**Drafting Note:** For systems with multiple integrated components (common in DPI), ensure that integration documentation covers all interfaces between components and with external systems. Link documentation acceptance to payment milestones to create appropriate incentives. The level of documentation detail should be calibrated to the technical capacity. For lower-capacity, Borrowers may want to specify that documentation should be written at a level accessible to non-specialist administrators and include step-by-step operational procedures.

#### **(IV) Interoperability and Portability**

**Rationale:** DPI systems are by definition shared digital building blocks that must interoperate with other government systems, private sector services, and potentially with systems in other jurisdictions. Annex A of this Guidance highlights the importance of specifying compliance with recognized open standards (such as ITU-T X.1281/OSIA for identity systems, OpenID Connect for authentication) to enable interoperability without mandating specific products. This clause translates these principles into enforceable contract provisions, ensuring that the system can exchange data, be migrated to alternative platforms, and operate within a broader DPI ecosystem.

#### **Example Contract Clauses:**

**Open Standards Compliance.** The System shall be designed, developed, and maintained in compliance with the open standards specified in the Terms of Reference. Where the Terms of Reference specifies compliance with a particular open standard (e.g., ITU-T Recommendation X.1281, OpenID Connect, OAuth 2.0, FHIR, or equivalent), the Contractor shall demonstrate compliance through testing and certification as specified. The System shall not require proprietary protocols, interfaces, or data formats for any function where an applicable open standard exists.

**API-Based Integration.** The System shall expose all core functionality through well-documented, standards-compliant Application Programming Interfaces (APIs). APIs shall

follow RESTful design principles or equivalent open standards and shall be documented in machine-readable formats (e.g., OpenAPI). The Contractor shall not implement integration mechanisms that create dependency on proprietary middleware, protocols, or connectors.

**Data Portability.** The System shall support the export of all Purchaser data—including configuration data, operational data, historical records, and metadata—in non-proprietary, industry-standard formats (e.g., CSV, JSON, XML, or formats specified in the Terms of Reference). Data export functionality shall be integrated to the System and shall be capable of producing complete, consistent, and usable data sets without the Contractor’s assistance or the use of proprietary tools.

**Platform Independence.** The System shall be designed to minimize dependency on specific hardware platforms, operating systems, or cloud service providers. Where the System is deployed on a cloud platform, the Contractor shall ensure that the architecture supports migration to alternative cloud providers or on-premise infrastructure without requiring redesign of core application components. The Contractor shall deliver a migration plan identifying all platform-specific dependencies and the steps required to migrate the System to an alternative environment.

**No Proprietary Lock-In.** The Contractor shall not introduce into the System any proprietary data formats, encryption schemes, or technical mechanisms that would prevent or unreasonably impede the Purchaser from: (a) accessing or extracting its own data; (b) migrating the System or its data to alternative platforms or service providers; (c) engaging alternative vendors to maintain, modify, or extend the System; or (d) integrating the System with other components of the Purchaser’s DPI ecosystem.

The Contractor shall, upon request, provide the Purchaser with a data portability and interoperability assessment report, identifying all data formats used, all external interfaces and standards implemented, and any limitations on data portability or system migration.

**Drafting Note:** Task teams should specify the applicable open standards in the Statement of Work based on the DPI domain: for digital identity systems, reference open standards (ITU-T X.1281, OpenID Connect) as described in Annex A; for health information, reference HL7 FHIR. The ‘no proprietary lock-in’ provision complements the guidance in the main body on distinguishing vendor lock-in from product lock-in—the goal is to prevent lock-in at the data and interface level, even where a specific product is selected.

## **(V) Right to Audit**

**Rationale:** The right to audit is essential for DPI systems that handle sensitive citizen data and public funds. For DPI procurement, the audit scope must be expanded to cover source code quality, security practices, system performance, data protection compliance, and adherence to open standards requirements. This broader scope reflects the heightened risks associated with foundational digital systems that serve entire populations.

### **Example Contract Clauses:**

**Scope of Audit Rights.** The Purchaser (or their designated representatives, including independent auditors and technical experts) shall have the right to examine, audit, and reproduce all Records related to the performance of this Contract. For the purposes of this Article, “Records” shall include, without limitation: (a) all financial records, books, documents,

accounting records, and payroll records; (b) all source code, object code, build scripts, and configuration files; (c) all solution architecture and design documentation; (d) all test plans, test results, and quality assurance reports; (e) information security and data protection policies, procedures, and incident records; (f) system performance logs, availability reports, and SLA compliance data; (g) records of compliance with open standards and interoperability requirements; and (h) subcontractor agreements, deliverables, and performance records.

**Technical and Security Audits.** The Purchaser shall have the right to conduct or commission, at its own cost, independent technical audits of the System, including: (a) source code reviews and security assessments (including penetration testing); (b) assessments of compliance with the open standards and interoperability requirements specified in this Contract; (c) data protection and privacy impact assessments; (d) performance and scalability testing; and (e) reviews of the Contractor's development practices, change management procedures, and quality assurance processes. The Contractor shall cooperate fully with such audits, including by providing access to development and testing environments, relevant personnel, and all requested documentation.

**Audit Access and Cooperation.** The Contractor shall make its Records, premises, systems, and personnel available for examination and audit at all reasonable times, upon reasonable notice (not less than ten (10) business days for routine audits and forty-eight (48) hours for urgent security-related audits). The Contractor shall provide the Purchaser's auditors with appropriate physical and logical access to systems, including read-only access to production and non-production environments as required for audit purposes.

**Retention Period.** The Contractor shall retain all Records for a period of five (5) years following the date of final payment under this Contract, or for such longer period as may be required by applicable law or regulation. This obligation shall survive the expiration or termination of this Contract.

**Remediation.** If an audit identifies material non-compliance with the requirements of this Contract, the Contractor shall, at its own cost, prepare and implement a remediation plan acceptable to the Purchaser within thirty (30) days of notification of the audit findings. The Purchaser shall have the right to verify the implementation of remedial actions through follow-up audits.

**Subcontractor Audit Rights.** The audit rights established in this Article shall extend to all subcontractors performing work under this Contract. The Contractor shall incorporate equivalent audit provisions into all subcontracts and shall ensure that the Purchaser has direct audit access to subcontractor records, systems, and personnel to the same extent as provided for the Contractor.

The failure of the Contractor to comply with the requirements of this Article shall constitute a material breach of this Contract.

**Drafting Note:** For DPI systems processing sensitive data (e.g., biometric identity data, financial transaction records), task teams should consider requiring periodic independent security audits (e.g., annually) as a contract obligation rather than merely reserving the right to audit. The audit clause should be read together with the data ownership clause (l)—the Purchaser's audit rights must be broad enough to verify that data ownership provisions are being respected. Where the system is hosted by a third-party cloud provider, ensure that audit rights extend to the cloud environment or that the cloud provider's own audit certifications (e.g., SOC 2, ISO 27001) are specified as requirements.



