



DIGITAL PUBLIC INFRASTRUCTURE AUDIT GUIDELINES

COMPTROLLER AND AUDITOR GENERAL OF INDIA

FOREWORD



Digital Public Infrastructure has emerged as the defining architectural choice of twenty-first century governance. Across the world, governments are deploying foundational digital systems - identity platforms, payment rails, data-exchange layers, and discovery networks - that now form the essential scaffolding upon which citizens access health, education, financial inclusion, and social protection. This shift is not merely technological. It is a structural reconfiguration of how the state exercises its obligations, distributes resources, and upholds rights at population scale.

The promise of Digital Public Infrastructure is real and significant. It enables the democratisation of services that were once accessible only to those with proximity, privilege, or connections. It brings transparency and traceability to public expenditure. It reduces systemic leakage and speeds up the delivery of entitlements. India's own experience through Aadhaar, the Unified Payments Interface, DigiLocker (a cloud-based platform for storage, sharing, verification of documents & certificates), and the Account Aggregator framework has demonstrated what is possible when foundational infrastructure is designed with openness, interoperability, and citizen-centricity at its core.

As with any large-scale public infrastructure, thoughtful design and sustained oversight are essential to ensure that benefits reach all segments of society. Considerations of accessibility, language diversity, digital literacy, and connectivity must remain integral to implementation. Similarly, the governance of data and institutional accountability mechanisms must evolve in step with technological progress, so that public trust remains firmly anchored. Data accumulated at scale requires robust governance frameworks to ensure that its use remains proportionate, transparent, and aligned with constitutional values and public interest.

It is precisely here that Supreme Audit Institutions have an indispensable role to play. Supreme Audit Institutions provide independent assurance that public resources are used efficiently, legally, and in public interest. In the digital era, this mandate extends naturally and necessarily to Digital Public Infrastructure. In the digital era, public audit correspondingly expands its lens, from financial regularity to systemic effectiveness, inclusion, and sustainability of digital systems built in public interest.

These Guidelines emerge from a recognition that auditing Digital Public Infrastructure requires a framework that is simultaneously technically rigorous and institutionally grounded; one that is faithful to the ISSAI standards that govern all SAI work, and sensitive to the cross-cutting, multi-actor, and rights-bearing character of DPI ecosystems. They have been developed in alignment with the United Nations Universal DPI Safeguards Framework (2024), which provides the global normative reference for what responsible DPI governance looks like in practice.

The People–Process–Tools & Technology–Data Governance framework that anchors these Guidelines is not merely a structural device; it embodies a deliberate and integrated approach to understanding Digital Public Infrastructure in its full institutional and technical context. The risks and outcomes associated with DPI cannot be meaningfully evaluated through a single audit perspective. They arise from the interaction of institutional capacity and accountability arrangements, governance and operational processes, system architecture and cybersecurity controls, and the complete data lifecycle, from creation and use to retention and disposal. Only by examining these dimensions collectively can audit move beyond isolated technical observations and produce findings that are coherent, proportionate, and capable of strengthening governance in practice.

I am pleased that these Guidelines have been developed with global applicability in mind, drawing on practices from India, Estonia, Singapore, Brazil, the European Union, and multilateral initiatives under the G20 and the UN Digital Economy agenda. They are intended to be of practical use for Supreme Audit Institutions across INTOSAI regions, all of whom are facing the same fundamental challenge: How to provide credible, evidence-based oversight of digital systems that are increasingly central to the governance compact between the state and its citizens. I commend all those involved in drafting these Guidelines and the various SAIs that provided inputs on the draft version of these Guidelines.

The credibility of digital transformation depends ultimately on the trust of the citizens it serves. Independent audit remains one of the most enduring instruments for sustaining that trust. These Guidelines are offered in that spirit, to reinforce confidence in digital transformation through principled, evidence-based oversight.



K Sanjay Murthy

Comptroller and Auditor General of India

New Delhi

PREFACE



These Guidelines have been prepared by the Office of the Comptroller and Auditor General of India to equip Supreme Audit Institutions with a structured, standards-aligned framework for auditing Digital Public Infrastructure. They respond to a clear and growing need: as governments worldwide deploy foundational digital systems at population scale, the demand for credible, independent oversight of those systems has grown correspondingly, yet the scale and complexity of DPI now calls for a more structured and integrated audit framework.

These Guidelines are designed for practical application. While grounded in internationally recognised principles of digital governance, they focus on operational clarity, enabling audit teams to plan, execute, and report DPI audits in a structured and proportionate manner.

The primary audience for these Guidelines is Supreme Audit Institutions engaged in performance, compliance, or information systems audits of Digital Public Infrastructure. They are equally relevant for SAIs conducting whole-of-government digital oversight, as well as for those building institutional capacity for DPI auditing for the first time. The Guidelines may also serve as a reference for regulators, data protection authorities, policymakers, and parliamentary oversight committees seeking to understand what a rigorous audit of DPI systems entails. Centres of excellence in public sector audit, including iCISA (the International Centre for Information System Audit, India), are expected to draw on these materials for training and professional development purposes.

Although developed reflecting India's extensive experience with large-scale DPI deployment, the Guidelines are drafted to be applicable across diverse national settings, DPI maturity levels, and legal frameworks. Calibrations for nascent, transitional, and mature DPI environments are embedded throughout.

The Guidelines are organised around four interconnected layers, each serving a distinct function in the audit framework: (i) ISSAI Standards (ISSAI 100, 3000, 4000, and GUID 5100) provide the mandatory professional foundation governing how DPI audits are planned, conducted, evidenced, and reported. (ii) The People–Process–Tools & Technology–Data Governance (PPT&D) Framework serves as the primary analytical lens through which all audit objectives, risks, criteria, and evidence are examined. Data Governance is treated as a full and equal fourth pillar of this framework, not a subordinate or cross-cutting dimension. (iii) The UN Universal DPI Safeguards Framework (2024) provides the content reference for evaluating DPI governance, its 18 principles and 13 risk categories, grouped under inclusion, safety, and structural integrity, inform the audit objectives and the risk assessment framework. (iv) ISO and other international standards (27001, 27701, 22301, 15489, 8000, 9241, WCAG 2.1, and OECD

principles) serve as specific control benchmarks within each PPT&D dimension. This layered architecture ensures professional consistency with ISSAI standards while providing substantive depth tailored to the governance and inclusion challenges inherent in DPI ecosystems.

The Guidelines are structured to support auditors through the full audit cycle. Chapters 1 through 4 build the conceptual and normative foundation: the context of DPI, the role of SAIs, the guiding PPT&D philosophy, and the international standards framework. Chapters 5 through 7 are the operational core: audit methodology, risk assessment, audit objectives and sub-objectives, and the Audit Design Matrix. Chapters 8 through 10 address institutional capacity, practical guidance for fieldwork, and the conclusion. The Annexures provide ready-to-use artefacts: a glossary, lifecycle mapping, an audit methodology diagram, a standards reference, a bibliography, and illustrative audit questions for both core DPI components (Annexure E) and sectoral applications (Annexure F).

These Guidelines complement existing ISSAI guidance on performance, compliance, and information systems auditing. They provide DPI-specific methodological support and do not override national laws, regulations, or SAI-issued instructions, which prevail where more stringent.

Given the rapidly evolving nature of DPI including AI integration, cross-border interoperability, and lessons from cooperative audits, these Guidelines are intended as a living document, subject to periodic review in consultation with INTOSAI bodies and partners. Feedback from applying institutions is encouraged.

These Guidelines have been prepared with the development process drew extensively on the INTOSAI Framework of Professional Pronouncements, the UN Universal DPI Safeguards Framework (2024), and comparative audit methodologies developed by SAI peers across ASOSAI, AFROSAI, and EUROSAI.

SAI India acknowledges partner SAIs of ASOSAI and domain experts whose feedback shaped successive drafts.

Shri Krishnan Sangaran Subramanian

Deputy Comptroller & Auditor General of India

(Human Resource, International Relations, Coordination & Legal)

TABLE OF CONTENTS

Executive Summary	9
1. Introduction	11
1.1 Context: Digital Transformation and Risks of Exclusion	11
1.2 Why DPI Matters for Inclusive Governance	11
1.3 Risks and Challenges	11
1.4 Role of Supreme Audit Institutions (SAIs)	11
1.5 Guiding Philosophy: People, Process, Tools & Technology and Data Governance Lifecycle (PPT&D)	12
1.6 Structure of the Guidelines and How to Use This Document	14
1.7 Summary of Key points	16
2. Digital Public Infrastructure – Context, Rationale, and Global Landscape	17
2.1 Defining Digital Public Infrastructure	17
2.2 Evolution of Service Delivery Models	18
2.3 Architecture of Digital Public Infrastructure	19
2.4 Safeguards, Inclusion and Trust	21
2.5 Global Cooperation and Regional Interoperability	22
2.6 Sectoral expansion beyond the Core Five	24
2.7 Value Proposition and Audit Relevance	25
2.8 Global and Regional Case Studies	27
2.9 Summary of Key points	28
3. Purpose and Scope of the Audit	29
3.1 Purpose of the Audit	29
3.2 Scope of the Audit	29
3.3 Lifecycle Coverage	30
3.4 Stakeholders in Audit	30
3.5 Mapping of Scope to People–Process–Tools & Technology and Data Governance	32
3.6 Audit Mandate, Jurisdiction and Period	33
3.7 Summary of Key points	35

4. International Standards and Frameworks	37
4.1 INTOSAI Framework: Foundational Principles and Standards	37
4.2 INTOSAI Guidance on Thematic Areas	38
4.3 ISO Standards: Security, Privacy, Continuity, and Accessibility	39
4.4 Data Protection and Privacy Frameworks	39
4.5 Open Data, Interoperability, and Competition	40
4.6 AI and Algorithmic Governance Standards	40
4.7 Accessibility and Inclusion Standards	41
4.8 Data Governance and Lifecycle Standards (Generic Framework)	41
4.9 National and Regional Adaptations	41
4.10 Summary of Key points	42
5. Audit Methodology	43
5.1 Integrated Audit Approach	43
5.2 Planning and Scoping	43
5.3 Data Collection and Evidence Techniques	44
5.4 Risk Assessment Framework	45
5.5 Summary of Key points	48
6. Audit Objectives and Sub-Objectives	49
6.1 Purpose of Defining Audit Objectives	49
6.2 Objective 1 – Governance of Digital Public Infrastructure	50
6.3 Objective 2 – Engagement with Stakeholders	52
6.4 Objective 3 – Inclusion, Access & Privacy for Citizens	54
6.5 Summary of Key points	56
7. Audit Design Matrix (ADM)	57
7.1 Purpose and Structure	57
7.2 Sample ADM Entries	57
7.3 Risk Rating and Severity	58
8. Capacity Building and Institutionalisation	61
8.1 Purpose	61
8.2 Competency Requirements for DPI Auditors	61
8.3 Institutionalising Audit-Ready DPI Processes	62
8.4 Tools and Technology Enablement	62
8.5 Continuous Professional Development (CPD)	63
8.6 Collaboration and Knowledge Sharing	63

8.7	Embedding the People-Process-Tools & Technology + Data Lens in Capacity Building	63
8.8	Expected Outcomes	64
9.	Auditing Digital Public Infrastructure (DPI): A Practical Audit Approach for SAIs	65
9.1	Purpose and Audience	65
9.2	What is DPI for Audit Purposes?	65
9.3	Audit Orientation: An Integrated Approach	66
9.4	Initial Scoping and Risk Assessment	66
9.5	Risk-Based Audit Planning	66
9.6	Jurisdiction, Accountability, and Public-Private Interfaces	67
9.7	Executing DPI Audits: Evidence and Methods	67
10.	Conclusion	69
11.	Annexures	71
11.1	Purpose of Annexures	71
11.2	Updating and Maintenance	71
	Annexure A – Glossary of Key Terms	72
	Annexure B – Mapping of DPI Processes to Data Lifecycle Phases	82
	Annexure C – Audit Methodology	83
	Annexure D – References and Bibliography	84
	Annexure E – Illustrative Audit Questions on Core DPI Components	85
	Digital Identity Systems	86
	Trust Infrastructure & Authentication	88
	Digital Payments Infrastructure	90
	Data Exchange and Interoperability Platforms	91
	Discovery & Fulfilment	92
	Annexure F – Illustrative Sectoral Audit Questions	95
	Health	96
	Education	97
	Agriculture and Rural Development	99
	Urban Governance & Smart cities	100
	E- Commerce & MSME Enablement	101
	Land and Property Registries	104
	Public Procurement & Supply Chains	106
	Taxation & Financial Management	108



EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Digital Public Infrastructure (DPI) is redefining how governments deliver essential services, exercise regulatory functions, and empower citizens in an increasingly digital economy. These infrastructures spanning digital identity systems, payments, data-exchanges, and service platforms form the foundational layer for inclusive growth and sustainable governance.

While the promise of DPI is profound, its risks are equally significant. Exclusionary design, inadequate accessibility, weak data governance, and absence of accountability mechanisms can erode trust and deepen social divides. As the stewards of public accountability, Supreme Audit Institutions (SAIs) have a critical role in ensuring that DPI initiatives embody the principles of equity, transparency, inclusion, and ethical data use.

This document provides a comprehensive audit framework for assessing Digital Public Infrastructure through the lens of People, Process, Tools & Technology, and Data Governance which anchors this guideline:

- **People** represent the *roles and responsibilities* across government, private sector, and citizen ecosystems;
- **Process** reflects the workflows and governance mechanisms that ensure *accountability*;
- **Tools & Technology** signify the *digital enablers* systems, APIs, registries, and analytical platforms that underpin DPI;
- **Data Governance** ensures that the use of data aligns with privacy, fairness, and inclusion principles.

Throughout, the Guidelines applies a Data Governance Lifecycle view covering data creation, use, sharing, retention, archival, and disposal ensuring that data is handled responsibly, lawfully, and ethically.

It enables SAIs and oversight institutions to evaluate whether DPI systems are designed, implemented, and operated in ways that safeguard citizens' rights, ensure inclusion, trust, efficiency, integrity, and resilience in service delivery.

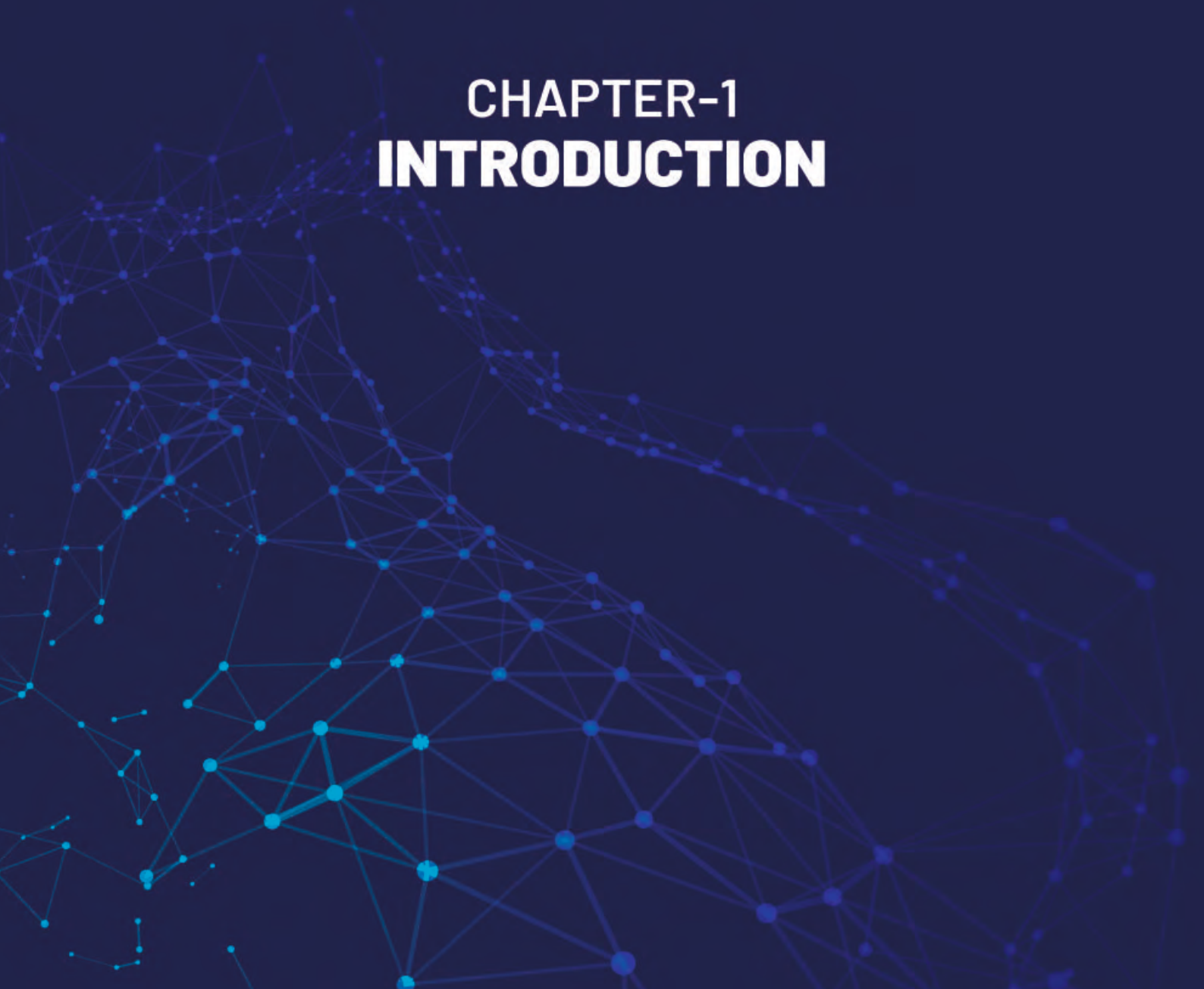
The Guidelines are grounded in the **ISSAI Framework of Professional Pronouncements (IFPP)** particularly:

- ISSAI 100: Fundamental Principles of Public Sector Auditing,
- ISSAI 3000: Performance Audit Standard,
- ISSAI 4000: Compliance Audit Standard, and
- GUID 5100: Guidance on Audit of Information Systems.

These are further aligned with United Nations Universal Digital Public Infrastructure Safeguards Framework and relevant ISO standards (27001 for information security, 27701 for privacy, 22301 for continuity, 9241 for accessibility, 8000 for data quality). Together, they ensure consistency with international good practices while maintaining flexibility for each SAI's national mandate.

This document is principally intended for Supreme Audit Institutions (SAIs) engaged in evaluating the governance, inclusiveness, and accountability of Digital Public Infrastructure (DPI) ecosystems. It may also be used as a reference by regulators, policymakers, and audit practitioners for strengthening governance, oversight, and accountability across DPI ecosystems. It may further be leveraged as a capacity-building resource by centres of excellence, such as iCISA (International Centre for Information System Audit, India), to support training and professional development.

By combining international audit standards with practical tools like the Audit Design Matrix (ADM), this Guideline aims to support SAIs in delivering high-quality, evidence-based audits that strengthen public trust in digital transformation.

An abstract graphic of a network or mesh structure, composed of numerous small blue dots connected by thin, light blue lines. The structure is more dense and complex on the left side, tapering off towards the right. It appears to be a stylized representation of a molecular structure or a data network.

CHAPTER-1 **INTRODUCTION**

CHAPTER-1

INTRODUCTION

1.1 Context: Digital Transformation and Risks of Exclusion

Governments worldwide are re-engineering public administration through Digital Public Infrastructure (DPI) foundational digital systems such as identity & registries, payments, authentication, and data-exchange layers. The Covid-19 pandemic accelerated this digital transformation, revealing both the power and the peril of digitisation. While DPI can democratize access to education, healthcare, finance, and justice, it can also unintentionally widen divides if design choices ignore affordability, accessibility, language, or connectivity. Citizens without digital literacy, assistive tools, or reliable networks risk being excluded from the very services meant to empower them.

1.2 Why DPI Matters for Inclusive Governance

DPI represents a structural shift from government-owned IT systems toward open, interoperable platforms that enable participation by citizens and private innovators alike. When well-governed, DPI can enhance service efficiency, lower costs, and enable rights-based access to data. When poorly governed, the risk of compromised privacy, entrenched bias, or monopolistic control of public digital goods may exist. Auditing DPI therefore becomes a matter not only of compliance but of public value assurance testing whether digital transformation truly advances equity and trust.

1.3 Risks and Challenges

Aligned with the principles outlined in the UN's Universal DPI Safeguards Framework which groups risks across inclusion, safety, and structural vulnerabilities such as governance, institutional weakness, and operational sustainability and consistent with the ISSAI 3000 (Performance Audit Standard) and GUID 5100 (Audit of Information Systems), auditors should recognise recurring risk themes under the DPI ecosystem which are Inclusion Risks, Design Risks, Data Governance Risks, Operational Risks and Accountability Risks. Additionally, Legal Risks run as a cross-cutting dimension across all five categories above. The detailed DPI risk categories are discussed in **Paragraph 5.4 - Risk Assessment Framework**.

Auditing these risks requires integrating performance, compliance, and IT perspectives to determine whether systems operate with economy, efficiency and effectiveness. In this context, due care may be taken to appropriately assess the issues related to equity and ethical integrity involved in the Digital Public Infrastructure landscape.

1.4 Role of Supreme Audit Institutions (SAIs)

Under ISSAI 100, ISSAI 3000 (Performance Audit), and ISSAI 4000 (Compliance Audit), Supreme Audit Institutions (SAIs) are mandated to ensure that governments act transparently, use public resources responsibly, and safeguard citizens' rights. In the digital era, this mandate extends to verifying:

- That Digital Public Infrastructure (DPI) initiatives comply with applicable legal, ethical, and data-governance standards; and

- That public-sector digitalisation enhances efficiency, effectiveness, accountability, and transparency rather than creating opacity.

SAIs therefore function as independent guardians of digital integrity, providing assurance that state digital infrastructures deliver value for money, operate lawfully, and serve all citizens fairly and inclusively.

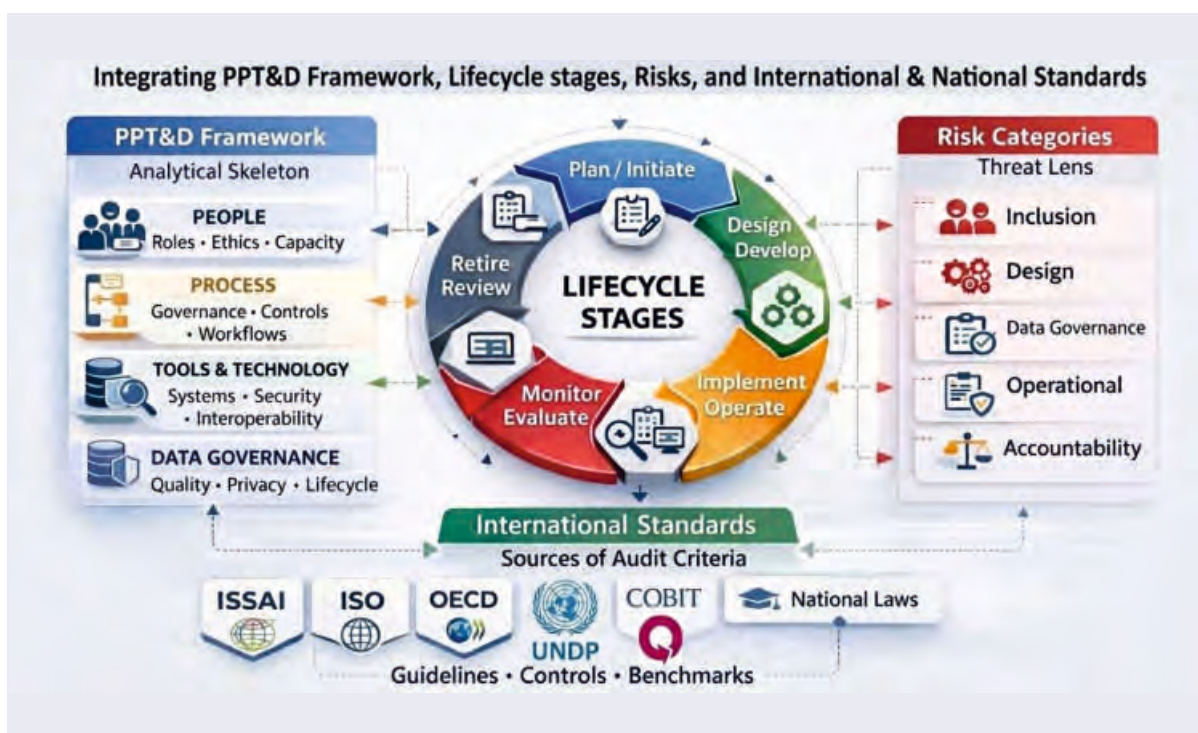
1.5 Guiding Philosophy: People, Process, Tools & Technology and Data Governance Lifecycle (PPT&D)

This Guideline is structured and interpreted through the People, Process, Tools & Technology, and Data Governance framework, which serves as the primary analytical spine for all stages of DPI auditing. All audit scope, objectives, risk assessments, criteria, and evidence are examined and integrated through this framework to ensure balanced coverage of:

- Institutional capacity (People),
- Governance mechanisms (Process),
- Technical systems (Tools & Technology), and
- Data lifecycle controls (Data Governance).

Other international frameworks and standards referenced in this document function as supporting sources of audit criteria within this overarching structure.

Figure 1: Framework for Digital Public Infrastructure (DPI) Audits



Data Governance is the fourth equal pillar of the PPT&D framework, with the same standing as People, Process, and Tools & Technology. Further, the governance lifecycle introduces the time dimension to the PPT&D framework.

While PPT&D provides the analytical structure, the lifecycle perspective captures how risks, controls, and outcomes evolve from system conception to decommissioning. Together, they

ensure that audits capture both technical soundness and societal and institutional impact. This integrated lens reflects the emphasis on evaluating systems rather than isolated transactions, recognising that accountability in the digital age resides in code, contracts, and organisational culture. In practical audit application, no DPI risk, control, or outcome should be assessed in isolation from the People, Process, Tools & Technology, and Data Governance dimensions. Auditors should use this framework to identify root causes, assess systemic interdependencies, and formulate evidence-based conclusions that link observed weaknesses or strengths to People, Process, Tools & Technology, and Data Governance factors across the DPI lifecycle.

The PPT&D framework is particularly useful for identifying Duplication, Fragmentation, Overlap, and Gaps (DFOG) across institutional mandates and data flows, enabling auditors to surface systemic governance weaknesses that may not be visible when examining any single agency or system in isolation.

Table 1: PPT&D Framework mapped to Focus and Key Audit Areas in DPI Audit

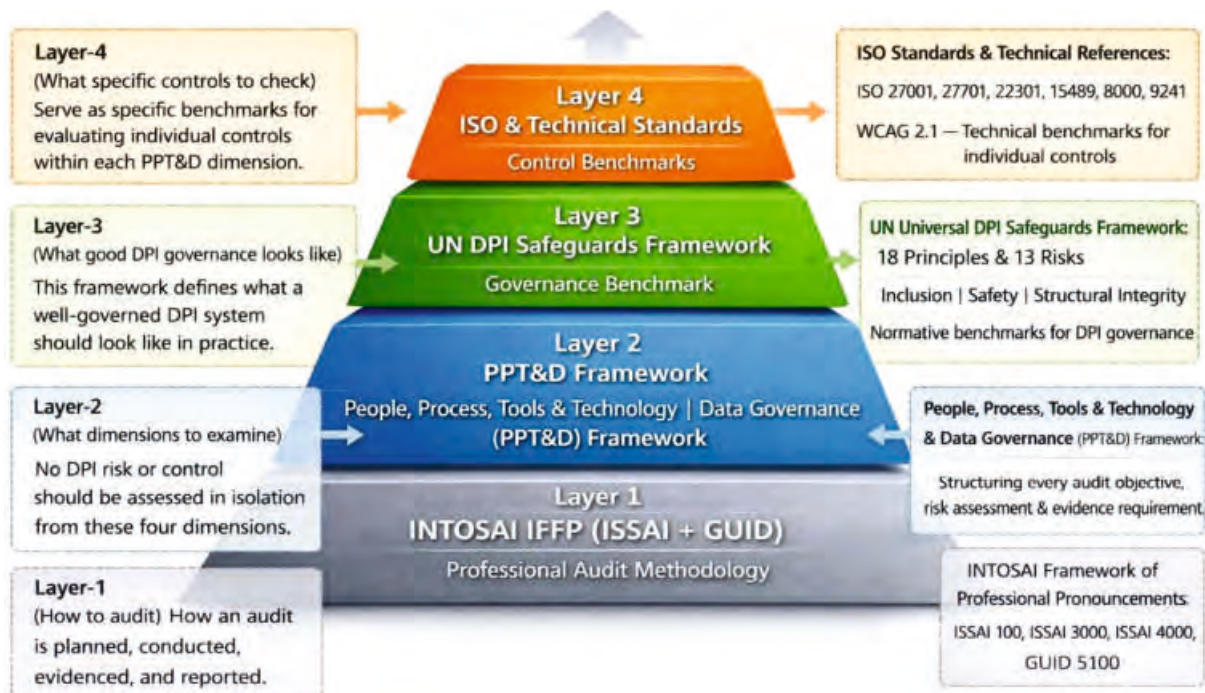
<i>Dimension</i>	Focus in DPI Audit	Key Audit Areas
<i>People</i>	Roles, responsibilities, competencies, and ethical conduct of institutions, vendors, regulators, and users	1. Governance structures and mandates; 2. Institutional roles and accountability lines; 3. Human resource capacity and training; 4. Ethics, conflict of interest, and integrity frameworks; 5. Oversight bodies and coordination mechanisms; 6. Stakeholder participation and representation; 7. Leadership and succession planning
<i>Process</i>	Governance workflows, policies, procedures, and control mechanisms governing DPI	1. Policy formulation and documentation; 2. Planning and budgeting processes; 3. Procurement and contracting; 4. Change and configuration management; 5. Grievance redressal and feedback systems; 6. Performance monitoring and reporting; 7. Compliance and internal control systems; 8. Inter-agency coordination procedures; 9. Risk management and audit follow-up

<i>Dimension</i>	Focus in DPI Audit	Key Audit Areas
<i>Tools & Technology</i>	Digital systems and technical infrastructure enabling DPI operations	1. System architecture and design standards; 2. Interoperability and open APIs; 3. Information security controls; 4. Authentication and identity systems; 5. Data exchange platforms and registries; 6. Business continuity and disaster recovery; 7. System performance and availability; 8. Vendor dependency and technology lock-in; 9. Configuration and access controls; Incident monitoring and response
<i>Data Governance Lifecycle</i>	Management of data from creation to disposal in line with legal, ethical, and proportionality principles	1. Lawful data collection and minimisation; 2. Consent management and user control; 3. Purpose limitation and access management; 4. Data sharing and third-party disclosures; 5. Storage security and retention schedules; 6. Archival and preservation mechanisms; 7. Data quality and integrity controls; Rights of access, correction, and erasure; 8. Deletion and disposal procedures; 9. Audit trails and life cycle documentation

1.6 Structure of the Guidelines and How to Use This Document

These Guidelines are built around four layered components, each serving a distinct purpose. Understanding this hierarchy will help auditors know where to look and what to apply at each stage of an audit.

Figure 2: The four layered components of the Guideline



The remaining chapters translate the guiding philosophy and audit dimensions outlined into a step-by-step framework for full cycle of DPI audits, as follows:

- **Chapter 2** situates Digital Public Infrastructure within global and regional practice, providing contextual understanding of DPI architectures, safeguards, and governance models relevant for audit scoping.
- **Chapter 3** defines the purpose, scope, lifecycle coverage, and stakeholder landscape of DPI audits, enabling auditors to determine audit boundaries, responsible entities, and priority areas.
- **Chapter 4** aligns audit criteria with international standards and legal frameworks, serving as the primary reference for assessing compliance, performance, and ethical data governance.
- **Chapter 5** sets out audit methodology, risk assessment approaches, and evidence-gathering techniques, guiding auditors in designing reliable and proportionate audit procedures.
- **Chapters 6 and 7** operationalise audit objectives through structured sub-objectives and the Audit Design Matrix (ADM), translating audit domains into testable questions, criteria, evidence sources, and risk assessments.
- **Chapters 8 to 10** address institutional capacity, reporting practices, and practical audit approaches, supporting consistent implementation, quality assurance, and continuous improvement of DPI audits.
- **The Annexures** provide illustrative sectoral and component-specific audit questions, templates, and reference materials for application in specific DPI contexts.

Together, these chapters guide auditors through a logical progression from strategic intent and risk identification to audit design, evidence collection, analysis, and reporting, consistent with the ISSAI doctrine of **principles → criteria → evidence → reporting**.

1.7 Summary of Key points

- Major DPI risk categories include Inclusion risks, Design risks, Data governance risks, Operational risks and Accountability risks. While Legal risks run as a cross-cutting dimension.
- The guideline uses the People, Process, Tools & Technology, and Data Governance (PPT&D) framework as the core analytical structure for DPI audits.
- Data Governance Lifecycle introduces the time dimension, ensuring audits examine how data is created, used, shared, stored, archived, and deleted.

An abstract graphic of a network or mesh structure, composed of numerous small blue dots connected by thin, light blue lines. The structure is more dense and complex on the left side, tapering off towards the right. It appears to be a stylized representation of a digital network or infrastructure.

CHAPTER-2

DIGITAL PUBLIC INFRASTRUCTURE – CONTEXT, RATIONALE, AND GLOBAL LANDSCAPE

CHAPTER-2

DIGITAL PUBLIC INFRASTRUCTURE –
CONTEXT, RATIONALE, AND GLOBAL LANDSCAPE

2.1 Defining Digital Public Infrastructure

Digital Public Infrastructure (DPI) refers to foundational digital systems and shared platforms that enable secure, inclusive, and interoperable digital transactions across government, private, and civic domains. A DPI typically combines five foundational categories¹ *i.e.* **identity, payment, data-exchange, trust infrastructure and discovery & fulfilment**, that together allow citizens and institutions to authenticate, pay, access services and share information safely and at scale.

As a governance-and-technology approach, DPI refers to a strategic approach for addressing socio-economic challenges at population scale by combining open, interoperable digital technologies with strong public governance frameworks. This approach is designed to enable broad-based participation, foster private and community-led innovation, and deliver inclusive public value across sectors such as financial inclusion, healthcare, education, climate action, access to justice, and social protection. DPI is now recognised as the new public utility of the digital age, comparable to roads or electricity networks in its societal importance. It provides the rails upon which digital services, such as welfare delivery, health insurance, tax, mobility, education, and e-commerce, can operate with reliability, speed, and reach. The concept has evolved from early e-government programmes into open, interoperable ecosystems where governments set standards, the private sector innovates, and citizens interact directly through trusted digital interfaces. Well-known examples include India's digital identity system **Aadhaar**, Brazil's instant payments platform **Pix**, and Estonia's secure data-sharing platform **X-Road**.

In essence, DPI encompasses both the philosophy of designing digital systems for public good at scale and the resulting foundational digital infrastructures that operationalise this philosophy in real-world governance contexts.

The global shift toward DPI accelerated in the aftermath of the COVID-19 pandemic, when governments needed to deliver benefits, health services, and payments rapidly and transparently. This experience demonstrated that digital foundations, once treated as optional, are now essential for resilience and inclusion. Multilateral bodies such as the UN, World Bank, and G20 have since adopted DPI as a pillar of digital-development strategy.

From an audit standpoint, DPI matters because it redefines the way public institutions store, process, and share information. It alters accountability relationships among people, processes, Tools & Technology, and data, requiring auditors to assess not only system performance but also governance, ethics, and equity. Effective DPI can expand access and trust; poorly governed DPI can amplify exclusion and risk.

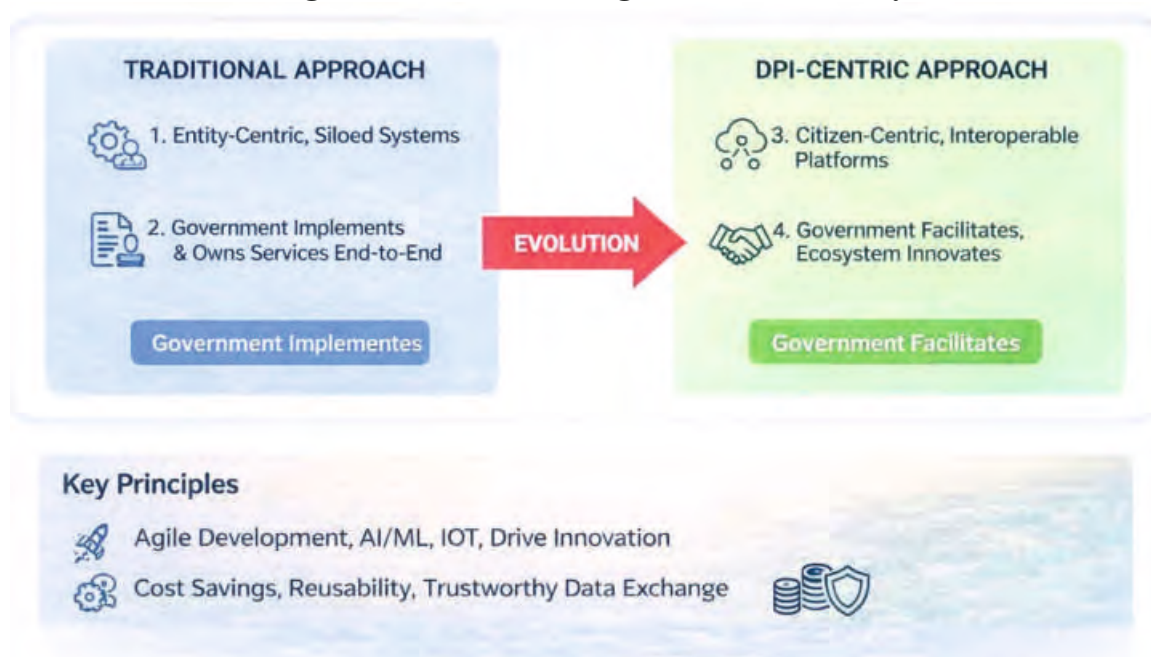
¹ Reference: DPI Wiki of Centre of Digital Public Infrastructure - CDPI (<https://cdpi.dev/>)

Therefore, the Guidelines treat DPI as both a technological construct and a governance paradigm, a combination that demands oversight for legality, efficiency, effectiveness, equity, and ethical integrity.

2.2 Evolution of Service Delivery Models

The concept of Digital Public Infrastructure has emerged from two decades of digital-governance reform and in the wake of the COVID-19 pandemic as mentioned in **Paragraph 2.1**. During that period, governments were compelled to deliver subsidies, health information, and mobility permissions to millions of citizens in real time. Those experiences underscored that digital systems are not simply administrative conveniences, they are critical national infrastructure. As a result, DPI is now recognised globally as a structural enabler of inclusive growth and governance resilience.

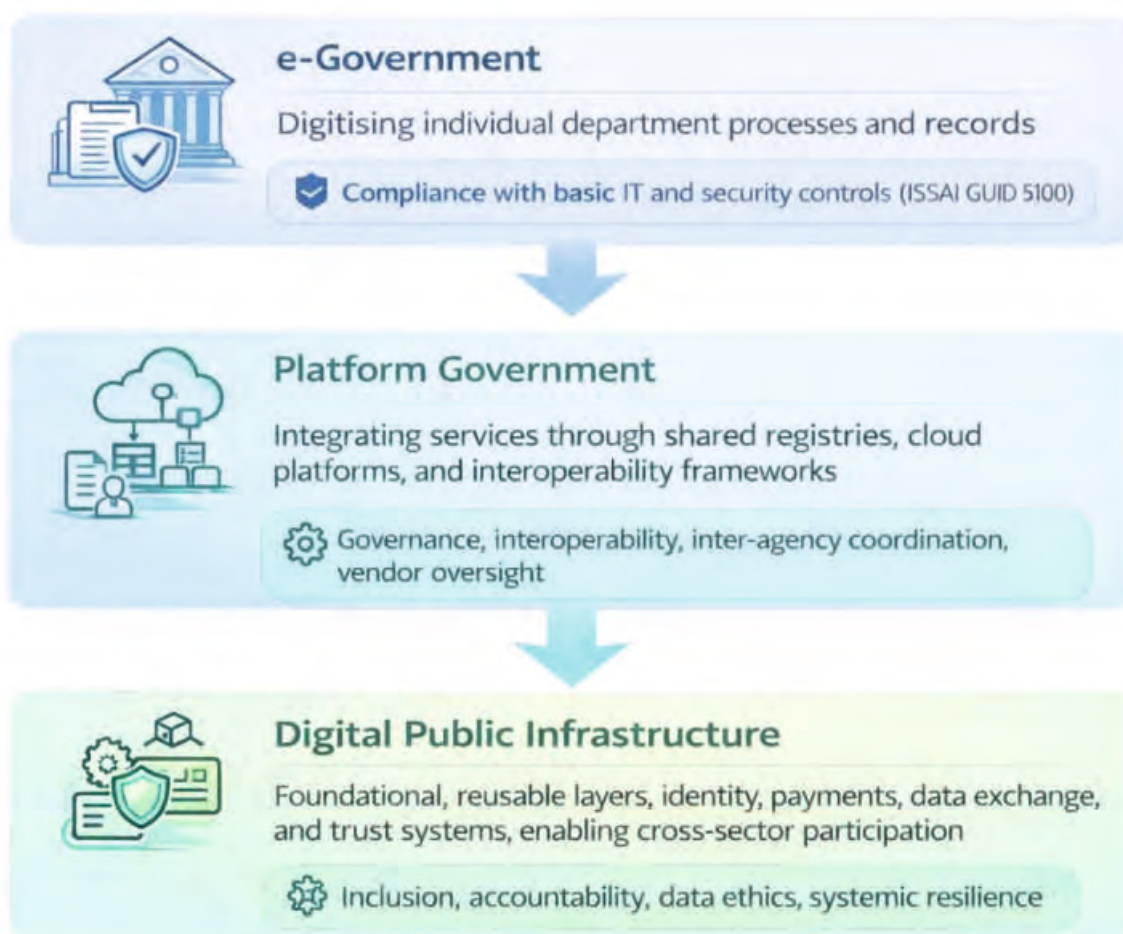
Figure 3: Evolution of Digital Service Delivery



The United Nations Development Programme (UNDP), the World Bank's Digital Economy Framework, and the G20 Digital Economy Working Group have all adopted DPI principles within their digital-transformation strategies. Common features across these initiatives include common design principles such as openness and interoperability, modular and federated architectures, privacy-by-design, and ethical data stewardship.

In parallel, regional alliances are shaping how DPI takes form. The European Union's eIDAS and DNS4EU initiatives promote cross-border digital identity and data sovereignty; ASEAN countries are building shared payment and identity rails; and African Union members are adopting open-source platforms such as MOSIP for interoperable digital identity. These collective efforts mark a shift from isolated IT projects toward federated digital ecosystems. The early stages of digital administration, commonly described as e-Government, focused on digitising departmental services. Subsequent Platform Government initiatives sought to consolidate those services on shared registries and clouds. Today's Digital Public Infrastructure stage connects entire sectors and stakeholders through common identity, transaction, and data-exchange layers. This progression can be summarised in Era with its Characteristics and Audit Focus for each as depicted in **Figure 4**.

Figure 4: The progression Era, Characteristics and Audit Focus



Each stage expands the state's fiduciary and ethical obligations toward data stewardship, citizen access, and systemic risk management.

2.3 Architecture of Digital Public Infrastructure

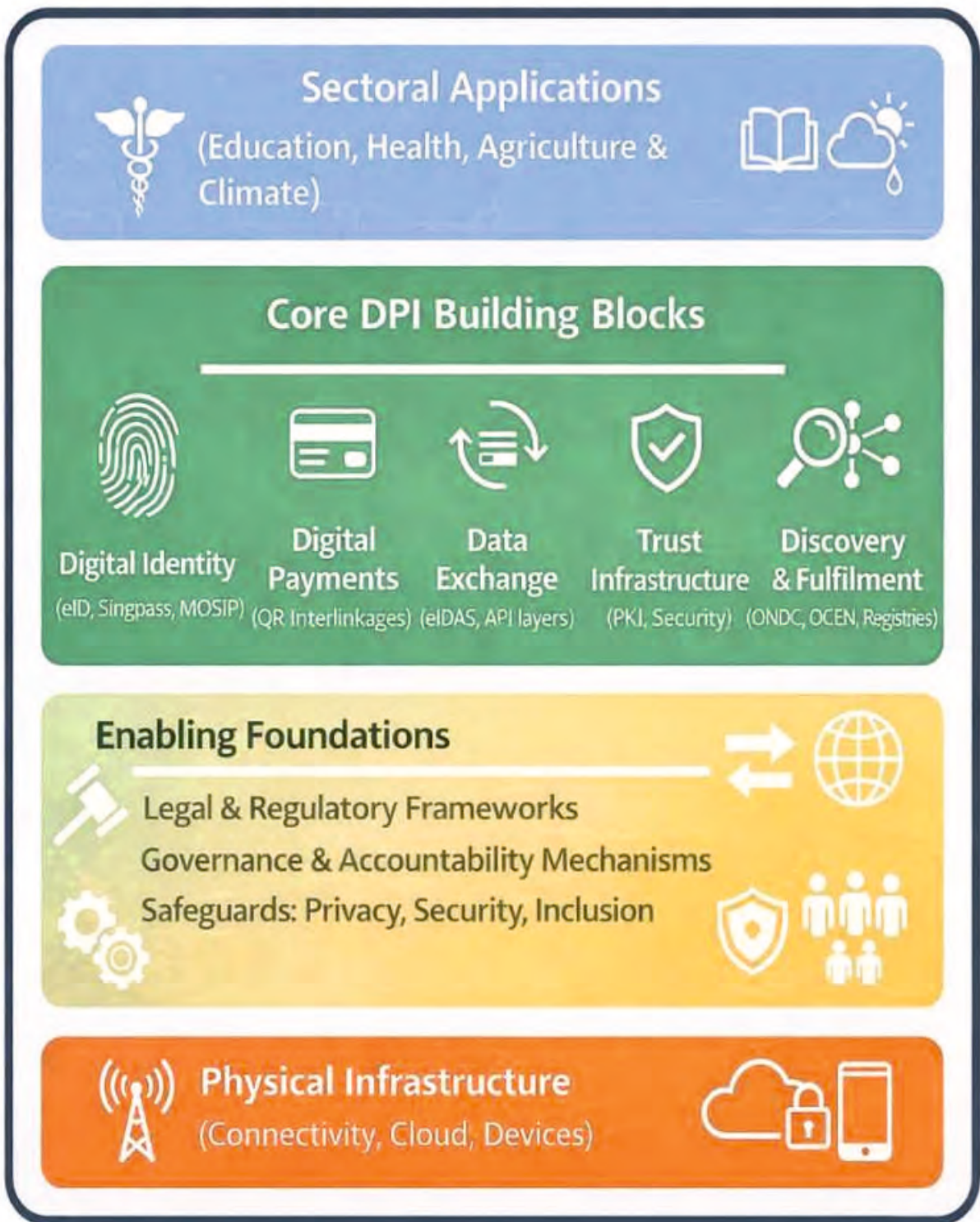
Digital Public Infrastructure operates as a **multi-layered architecture** that connects people, processes, and technology through secure data flows. The architecture of DPI is based on the principle of *shared, reusable, and interoperable building blocks* that enable citizens and service providers to transact securely within a governed ecosystem.

At its heart are two registries:

- Citizen Registry:** Each individual is uniquely identifiable through a trusted digital identity. Authentication may rely on biometrics, demographic data, or federated identity systems, but the goal is the same *i.e.* to ensure that individuals can securely access services across multiple platforms.
- Service Provider Registry:** Public and private entities seeking to deliver services on the DPI must be registered and authenticated. This typically requires submission of statutory credentials (*e.g.*, company registration, tax ID) and adherence to eligibility criteria established by the DPI's governing authority.

While configurations differ across countries, most DPI ecosystems share four interdependent layers:

Figure 5: Independent Layers of DPI ecosystem

**(a) Physical Infrastructure Layer – Connectivity and Compute**

This foundational layer provides the technical substrate required for DPI to function. It includes telecommunications networks, data centres, cloud infrastructure, end-user devices, and basic cybersecurity controls. Reliability, scalability, and resilience at this layer are prerequisites for all higher-level DPI components.

(b) Enabling Foundations (Governance Layer) – Rules, Safeguards, and Oversight

This layer **establishes the institutional and regulatory environment** within which DPI operates. It defines policies, standards, and accountability mechanisms to ensure trust, interoperability, and protection of citizen rights. Key elements include: Legal and regulatory frameworks, Data classification and data-sharing policies, Consent management and grievance redressal mechanisms, Privacy, security, and inclusion safeguards aligned with standards such as ISO/ IEC 27001 and ISO/ IEC 27701. This layer governs *how* DPI is built, used, and supervised.

(c) Core DPI Building Blocks – Foundational Digital Platforms

This layer provides the shared, reusable digital capabilities that act as common rails across sectors. These building blocks are sector-agnostic and enable trust and interoperability at population scale. They typically include: **Digital Identity** (e.g., eID, Authentication services), **Digital Payments** (Interoperable payment rails), **Data-Exchange** (Consent-based data sharing, APIs), Trust Infrastructure (PKI, digital signatures, security services), **Discovery and Fulfilment** (Registries, Directories, ONDC-like components)

Together, these components form the **trust architecture** of the digital ecosystem.

(d) Sectoral Applications (Experience Layer) – Service Delivery Interfaces

This top layer consists of sector-specific applications and platforms built on top of the core DPI building blocks. These include systems for health, education, agriculture, climate services, urban governance, and digital commerce. Citizens, businesses, and institutions interact with DPI primarily through this layer *via* portals, mobile apps, assisted service centres, and APIs. Inclusive design principles, such as WCAG 2.1 accessibility standards, multilingual support, and usability norms (e.g., ISO 9241) are critical here to ensure equitable access.

Together, these layers form an open yet secure ecosystem that enables real-time, data-driven governance while maintaining transparency and accountability.

This layered architecture is not only a technical construct but a governance model. It enables transparency through open standards, inclusion through accessible interfaces, and accountability through verifiable audit trails. Understanding this architecture is essential for auditors when planning DPI engagements or defining scope and evidence requirements.

2.4 Safeguards, Inclusion and Trust

The promise of Digital Public Infrastructure depends on the degree of trust it inspires among citizens. Trust arises when systems are secure, transparent, and inclusive and erodes rapidly when exclusion, opacity, or misuse of data occurs. Therefore, the design and oversight of DPI must integrate legal, technical, and ethical safeguards from the outset.

At the policy level, safeguards ensure that participation in digital ecosystems remains voluntary, informed, and equitable. This includes clear consent frameworks, grievance redressal channels, and options for assisted or offline access. At the technical level, safeguards encompass strong authentication, encryption, and differential-privacy measures that protect personal information while preserving service efficiency. At the institutional level, independent regulators, data-protection authorities, and audit institutions reinforce accountability.

Around the world, governments are discovering that inclusion cannot be retrofitted. Barriers such as affordability, connectivity, language, disability, and digital literacy must be addressed during system design. Global good-practice frameworks including the UN's Universal DPI Safeguards Framework, UN Convention on the Rights of Persons with Disabilities (CRPD), WCAG 2.1, and ISO 9241 on human-centred design provide reference criteria for accessible interfaces and equitable participation.

Data governance is the second pillar of trust. Transparent data-collection policies, purpose limitation, minimal-data principles, and retention schedules aligned with ISO 27701 and ISO 15489 are essential to maintain legality and legitimacy. Ethical use of algorithms, bias testing, and explainability further extend these safeguards into the domain of artificial intelligence.

For auditors, these safeguards translate into audit criteria that measure not only compliance with law but also fairness and proportionality in practice. An effective DPI audit therefore examines whether:

- Safeguards are embedded at each phase of the data lifecycle
(**Creation → Use → Sharing → Retention → Disposal**); and
- Institutional mechanisms exist to monitor, report, and correct breaches that threaten inclusion or trust.

Inclusion, accessibility, and ethical integrity are thus not peripheral concerns, they define the legitimacy and sustainability of DPI itself.

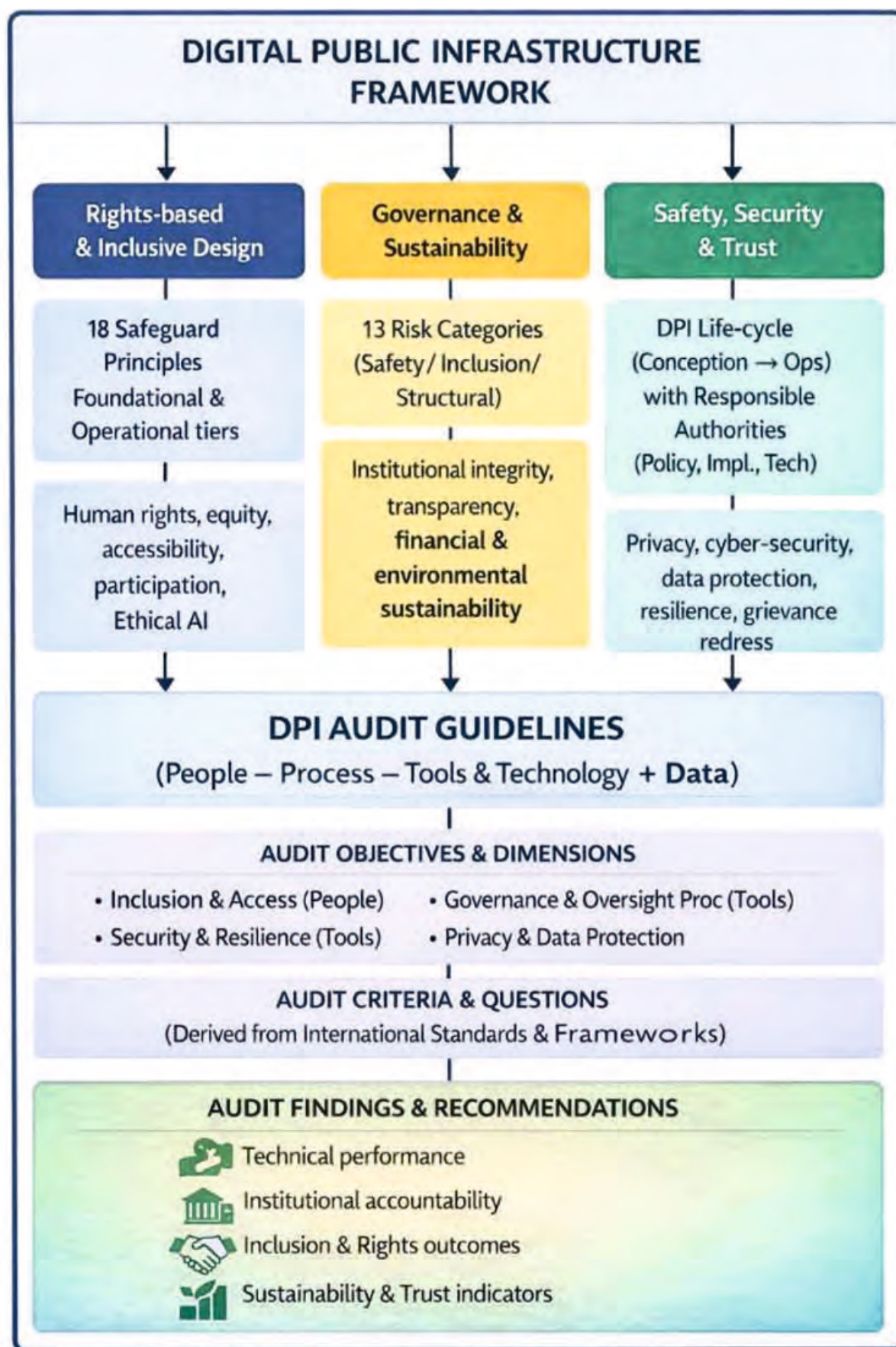
2.5 Global Cooperation and Regional Interoperability

The momentum around Digital Public Infrastructure has moved from isolated national projects to coordinated international efforts. Multilateral organisations such as the **United Nations (UN)**, the **World Bank**, and the **G20 Digital Economy Working Group** have endorsed DPI as a foundation for inclusive digital transformation. These frameworks emphasise openness, interoperability, safeguards, and accountability as common design principles.

The United Nations developed comprehensive **Universal DPI Safeguards Framework (2024)** to guide the design and governance of digital systems that serve the public interest safely, inclusively, and sustainably. The document sets out 18 foundational and operational principles and 13 interrelated risks, grouped under three broad categories *i.e. inclusion, safety, and structural vulnerabilities* covering the entire DPI life cycle from conception and design through development, deployment, and operation. They address issues of privacy, vulnerability, digital insecurity, discrimination, weak institutions, and long-term sustainability. While the Framework's formal structure rests on these risk categories, its recommendations emphasise three recurring themes: **Rights-based and inclusive design** – embedding equality, accessibility, and human rights in digital systems; Governance and sustainability ensuring transparent institutions, accountability, and durable financing; and Safety, security, and trust integrating privacy, cybersecurity, and ethical-use safeguards from the outset.

The **Digital Public Infrastructure Alliance**, launched during India's G20 presidency, has provided a global platform for knowledge exchange and capacity building among governments, development agencies, and standard-setting bodies. This collaboration enables countries to adapt open building blocks such as **MOSIP** (Modular Open Source Identity Platform) and **Beckn Protocol** (for interoperable digital commerce) according to national contexts while maintaining global compatibility.

Figure 6: Alignment Map between DPI Safeguards Framework and DPI Audit Guidelines



This Audit Guidelines aligns with the UN approach through its People, Process, Tools & Technology and Data Governance dimensions. This alignment ensures that audits of DPI evaluate not only technical efficiency and reliability but also equity, accountability, sustainability, and human-centred digital transformation, in line with international standards and commitments under the **UN Global Digital Compact** and the **G20 Leaders' Declaration (2023)**.

Regional cooperation is reinforcing these global ambitions.

- In Europe, the eIDAS 2.0 Regulation, the European Digital Identity Wallet, and the DNS4EU project aim to create secure, sovereign digital infrastructure for cross-border transactions.
- In Southeast Asia, the ASEAN Digital Masterplan 2025 promotes cross-border data flows, interoperable payment systems, and mutual recognition of digital identities.
- Across Africa, initiatives such as the Smart Africa Alliance and MOSIP adoptions are supporting federated identity and payment systems to advance regional inclusion.
- In Latin America, countries such as Brazil and Chile are building open data-exchange layers and digital ID systems inspired by DPI principles.

These cooperative mechanisms reflect a broader understanding that **digital sovereignty** and **interoperability** can coexist when guided by transparent governance. Instead of isolated national platforms, nations are now building **federated, standards-based digital ecosystems** that allow secure data-exchange while respecting local laws and privacy frameworks.

From an audit perspective, regional cooperation presents both opportunity and complexity. Shared digital infrastructure requires alignment of audit criteria across jurisdictions covering data protection, cybersecurity, and service continuity. Supreme Audit Institutions (SAIs) can therefore benefit from peer learning and cooperative audits under INTOSAI's Working Group on IT Audit (WGITA) and regional bodies such as **ASOSAI** and **AFROSAI**. Such joint audits help establish comparable benchmarks for digital inclusion, resilience, and accountability.

Understanding these global and regional trends allows auditors to evaluate DPI systems not in isolation but as part of an interconnected international digital ecosystem where interoperability, ethics, and inclusion are shared responsibilities.

2.6 Sectoral expansion beyond the Core Five

Although the **foundational architecture** of Digital Public Infrastructure is often described through five core layers *i.e. identity, payments, data-exchange, trust infrastructure, and discovery & fulfilment*, many governments are now extending these capabilities into **sector-specific ecosystems**. This evolution reflects the growing maturity of digital governance and the need to embed DPI principles of openness, interoperability, decentralisation, inclusion, and accountability across all domains of public life.

Health: National health platforms such as India's *CoWIN* and the *Ayushman Bharat Digital Mission*, Singapore's HealthHub, and the EU's European Health Data Space demonstrate how DPI principles enable secure vaccination tracking, electronic health records, and portability of care. Auditors must evaluate data-sharing governance, consent, and reliability of health registries.

Education: Platforms like *DIKSHA* in India and *Open Edu* in the EU use common digital identity and content-interoperability standards to ensure that learning materials reach diverse communities. Key audit concerns include accessibility, content quality, and intellectual-property safeguards.

Digital Commerce and MSME Enablement: Initiatives such as the *Open Network for Digital Commerce (ONDC)* in India and *Beckn-protocol-based platforms* apply DPI logic to marketplaces, ensuring open participation and vendor neutrality. Auditors assess fairness of algorithms, transparency in transaction recording, and consumer-protection compliance.

Climate and Sustainability: Emerging DPI applications support carbon-credit tracking, environmental data-exchanges, and renewable-energy registries. These require strong data-quality standards (ISO 8000) and traceability mechanisms.

Urban and Mobility Services: Smart-city platforms integrate transportation, utilities, and emergency services through common APIs and geospatial data layers. Auditors examine interoperability, cyber-resilience, and inclusiveness for differently-abled citizens.

Sectoral DPI ecosystems thus extend the original digital-public-goods philosophy into new policy spaces. They amplify both benefits (efficiency, inclusion, innovation) and risks (privacy breaches, exclusion, monopolistic behaviour). From an audit perspective, this expansion underscores the importance of **whole-of-government assurance frameworks** that verify consistency of standards, equity, and ethical use of data across sectors.

2.7 Value Proposition and Audit Relevance

Digital Public Infrastructure delivers value on multiple fronts *i.e.* for citizens, governments, and markets by providing a trusted digital foundation that reduces friction, lowers cost, and expands inclusion. Its success depends not only on technology but on governance that ensures equity, security, and ethical integrity.

(a) For Citizens and Communities

- Provides secure digital identities and verifiable credentials that enable access to welfare, education, health, and financial services.
- Reduces transaction costs, travel time, and paperwork through paper-less, cash-less, and presence-less interactions.
- Strengthens agency and trust when citizens control their own data through consent dashboards and grievance mechanisms.

(b) For Government and Public Institutions

- Enables integrated policy delivery and better targeting of subsidies and benefits.
- Improves transparency through real-time data and open dashboards.
- Allows interoperability across departments, cutting duplication and manual reconciliation.
- Creates a foundation for evidence-based policymaking through reliable, high-quality data.

(c) For Private Sector and Innovation Ecosystem

- Provides open, non-discriminatory rails that lower barriers for startups and service providers.

- Encourages competition and innovation through open-API standards rather than closed proprietary systems.
- Stimulates digital-economy growth and job creation while preserving public oversight.

From an Audit Perspective

For auditors, DPI represents a **shift in the locus of accountability**, from single-agency projects to multi-actor digital ecosystems. Consistent with ISSAI 3000 performance audit principles, traditional audit approaches must therefore adapt to evaluate whether public value is being delivered across all dimensions:

- **Economy** – Are resources used efficiently to build shared and interoperable digital infrastructure instead of siloed solutions?
- **Efficiency** – Are processes automated and standards-driven to minimise manual effort and error, while enabling coordinated participation across ecosystem actors?
- **Effectiveness** – Are the intended policy and service outcomes achieved?
- **Equity** – Do systems reach all segments of society without bias or exclusion?
- **Ethical Integrity** – Are privacy, transparency, and fairness upheld in data use and algorithmic design, with safeguards against misuse and violations of due process?

Evaluating this value proposition requires an integrated audit view that links People, Process, Tools & Technology, and Data Governance. The Audit Design Matrix (ADM) developed later in these Guidelines translates these dimensions into measurable criteria and evidence sources. By verifying the public value of DPI, auditors help strengthen citizen trust and reinforce the legitimacy of digital governance itself.

As DPI systems expand across sectors, auditors may also consider whether governance arrangements, data protection safeguards, and accountability mechanisms are applied consistently across sectoral implementations, so that citizens receive comparable protections and obligations regardless of the sector in which DPI is deployed.

Table 2 provides a risk–value linkage that maps each DPI risk category to the public value dimensions.

Table 2: Mapping DPI risk categories to the public value dimensions.

Risk Category	Economy	Efficiency	Effectiveness	Equity	Ethical Integrity
Inclusion Risks	●	●	✓	✓	✓
Primary Audit Focus: Coverage of vulnerable and marginalised groups, geographic and socio-economic access barriers, affordability, assisted access models, exclusion risks in enrolment and service delivery.					
Design Risks	●	●	✓	✓	✓
Primary Audit Focus: Algorithmic bias, opaque or automated decision-making, accessibility of user interfaces, human-centred design, exclusion due to technology choices.					
Data Governance Risks	●	✓	✓	●	✓
Primary Audit Focus: Consent mechanisms, data minimisation and retention, privacy protection, surveillance risks, secure and purpose-bound data sharing, interoperability controls.					
Operational Risks	✓	✓	✓	●	●
Primary Audit Focus: Vendor lock-in, continuity and resilience planning, dependency on single actors, cybersecurity preparedness, systemic stability and long-term sustainability.					
Accountability Risks	✓	●	✓	✓	✓
Primary Audit Focus: Clarity of ownership and responsibility across public–private actors, rule-of-law safeguards, monopoly risks, grievance redress mechanisms, auditability and enforceability.					

✓ = Direct relevance

● = Indirect relevance

2.8 Global and Regional Case Studies

The practical application of Digital Public Infrastructure varies across countries, reflecting different institutional and legal frameworks. Yet, a common design philosophy of open standards, interoperability, user-centric design, and accountability through auditable data trails links them all.

(a) India Stack

A comprehensive ecosystem comprising *Aadhaar* (digital identity), *UPI* (unified payments interface), *DigiLocker* (secure document repository), and *Account Aggregator* frameworks. India Stack exemplifies how open APIs and layered architecture can scale service delivery to hundreds of millions while enabling private-sector innovation. Audit focus areas include authentication-reliability, grievance-redressal, and data-protection compliance.

(b) Estonia's X-Road

A decentralised, open-source data-exchange system linking government and private databases. Each data transaction on X-Road is digitally signed and logged, ensuring traceability and accountability. Audit concerns include cybersecurity resilience, incident monitoring, and continuity of inter-agency governance.

(c) Singapore's SingPass and MyInfo

A federated digital-identity system that allows citizens and residents to access over 400 government and private services through a single secure login. *MyInfo* enables consent-based data sharing between agencies, reducing redundancy. Audit considerations include consent management, vendor oversight, and cross-sector data integrity.

(d) European Union's eIDAS 2.0 and European Digital Identity Wallet

The EU's cross-border trust framework ensures mutual recognition of electronic identities, signatures, and seals among member states. The new European Digital Identity Wallet extends control to citizens, who can store credentials locally while remaining interoperable across jurisdictions. Key audit areas include interoperability governance, privacy assurance, and conformity with data-protection law.

(e) MOSIP (Modular Open-Source Identity Platform)

A global open-source initiative inspired by India's DPI model but adopted independently by countries such as the Philippines, Morocco, and Ethiopia. MOSIP allows nations to build secure, sovereign identity systems without vendor lock-in. Audit considerations include security governance, localisation, and adaptation to national privacy laws.

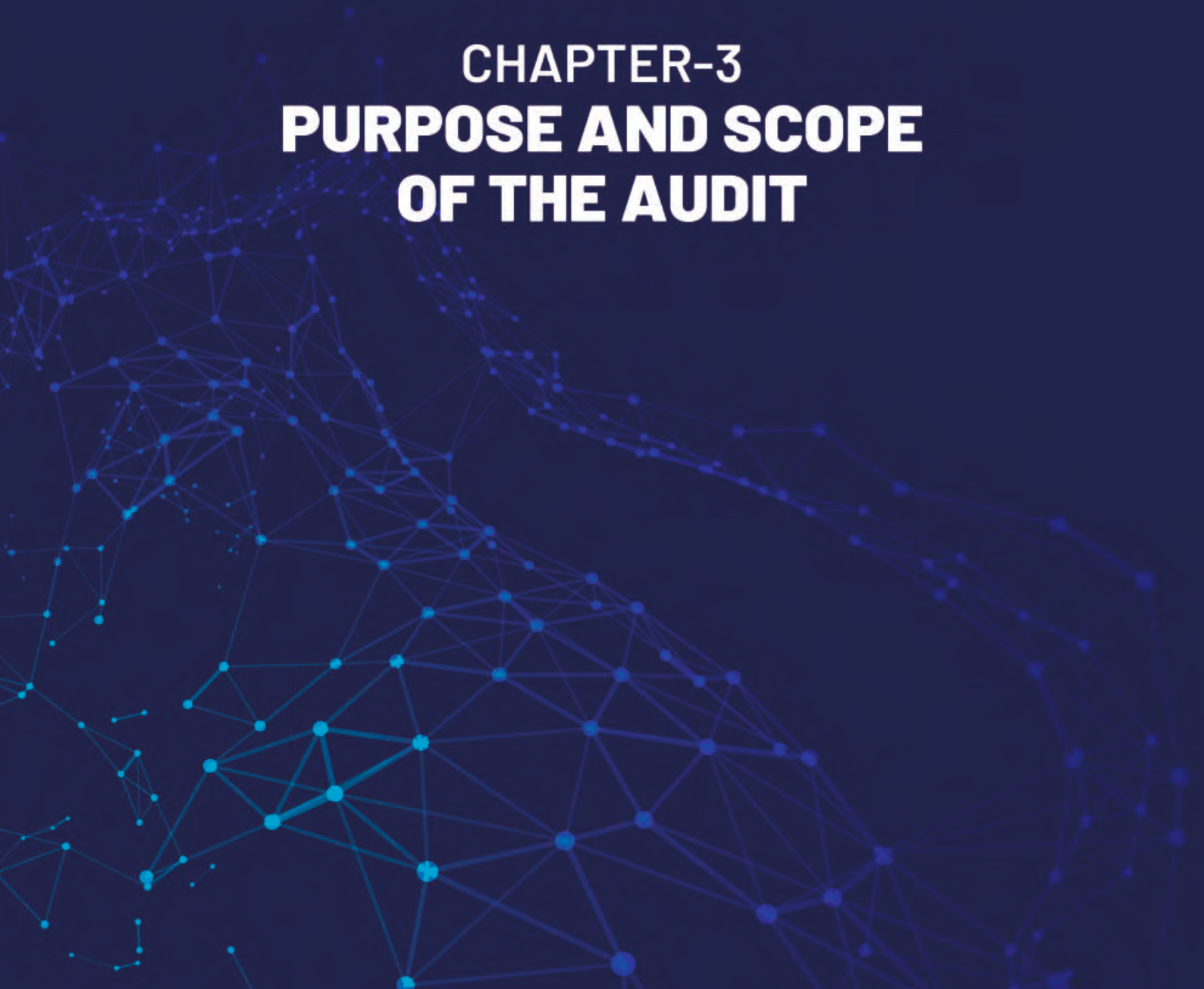
(f) Regional and Multilateral Initiatives

Projects such as the *Smart Africa Alliance*, *ASEAN Digital Masterplan 2025*, and *Digital Public Infrastructure Alliance* (launched under the G20) are promoting south–south cooperation, shared standards, and capacity building. These partnerships highlight the growing recognition that DPI success depends on collective governance and mutual accountability.

Collectively, these examples illustrate that DPI is not a singular model but a **framework of interoperable, auditable, and citizen-centric systems**. For auditors, comparative analysis of such implementations provides valuable benchmarks on governance maturity, data ethics, and inclusion.

2.9 Summary of Key points

- **Digital Public Infrastructure (DPI)** consists of foundational digital systems that enable secure and interoperable digital transactions, typically built around **identity, payments, data exchange, trust infrastructure, and discovery & fulfilment**.
- Digital governance has evolved from **e-Government** → **Platform Government** → **Digital Public Infrastructure**, moving from isolated departmental systems to interconnected digital ecosystems.
- **Trust and inclusion are central to DPI success**, requiring safeguards such as strong data protection, consent mechanisms, accessibility standards, and grievance redressal systems.
- DPI principles are expanding beyond the core digital rails into **sectoral ecosystems** such as **health, education, digital commerce, climate data systems, and smart-city services**.
- From an **audit perspective**, DPI requires evaluating not only technical performance but also **economy, efficiency, effectiveness, equity, and ethical integrity** across complex multi-stakeholder digital ecosystems.

An abstract graphic in the bottom-left corner of the page, consisting of a complex network of interconnected nodes and lines. The nodes are represented by small circles in various shades of blue and cyan, while the lines are thin and light blue. The network structure is dense and irregular, resembling a molecular or digital web, and it extends diagonally across the lower portion of the cover.

CHAPTER-3

PURPOSE AND SCOPE OF THE AUDIT

CHAPTER-3

PURPOSE AND SCOPE OF THE AUDIT

3.1 Purpose of the Audit

Digital Public Infrastructure (DPI) audits aim to assess whether governments design, implement, and operate digital platforms and shared digital systems within a broader ecosystem of public and private actors in accordance with the principles of inclusion, equity, accountability, and transparency.

The audit therefore seeks to:

- Evaluate whether DPI initiatives promote inclusive and equitable service delivery;
- Determine whether governance structures and controls ensure privacy, security, accountability, and effective oversight;
- Verify that data management practices adhere to global standards of lawfulness, fairness, and proportionality throughout the data lifecycle;
- Assess whether DPI systems achieve intended outcomes efficiently and sustainably.

The audit framework applies a People, Process, Tools & Technology, and Data Governance perspective across these objectives to enable systematic assessment of institutional arrangements, operational processes, technical systems, and information governance.

3.2 Scope of the Audit

The scope of DPI auditing extends beyond individual applications to the entire enabling ecosystem including legislation, governance frameworks, architecture, and operational processes. It encompasses:

1. **Processes** – governance and operational mechanisms spanning planning, procurement, design, implementation, maintenance, and oversight, incorporating the UN Universal DPI Safeguards Framework's principles of inclusion, safety, and sustainability at each stage;
2. **Lifecycle phases** – coverage of all stages of the DPI lifecycle, from *conception and design through development, deployment, operation, decommissioning, and archival*, ensuring continuous monitoring, learning, and adaptation;
3. **Actors** – all responsible authorities as defined in the UN Framework being the policy, implementing, and oversight bodies, along with regulators, service providers, vendors, and users, each accountable for transparency, participation, and redress; and
4. **Domains** – the core DPI layers of identity, payments, data exchange, and trust infrastructure, as well as sectoral extensions such as health, education, commerce, environment, and social protection, where DPI principles of openness, interoperability, and human rights-based design are applied. Regardless of mandate, all DPI audits should aim to assess whether the governance and safeguards are in place; systems operate effectively, securely, and inclusively; and data are managed lawfully, ethically, and efficiently across their lifecycle.

3.3 Lifecycle Coverage

To ensure holistic evaluation, DPI audits should mirror the **lifecycle approach** endorsed by GUID 5100 (Audit of Information Systems) and UN Universal DPI Safeguards Framework.

Table 3: Typical DPI lifecycle and corresponding audit concerns

Lifecycle Phase	Key Audit Focus	Example Evidence
Conception & Design	Policy intent, stakeholder consultation, impact assessment, system architecture principles, interoperability and scalability planning	Concept notes, design documents, stakeholder meeting records
Development & Procurement	Vendor selection, contractual transparency, adherence to standards, IP and data ownership, security-by-design, change control mechanisms	Tender documents, contracts, technical specs
Deployment & Operations	System testing, operational readiness, accessibility compliance, cybersecurity management, disaster recovery and continuity arrangements, data protection controls	Test reports, accessibility audits, incident logs, DR/ BCP plans
Maintenance & Continuous Improvement	Grievance resolution, feedback loops, version control, system upgrades, risk monitoring, staff capacity building	Service tickets, update logs, citizen feedback, risk registers
Decommissioning/ Archival	Data retention, disposal, legacy management	Archival policy, deletion certificates

3.4 Stakeholders in Audit

DPI ecosystems involve a **multi-actor governance model** often crossing institutional and sectoral boundaries.

Figure 7: Interactions and the Stakeholders of DPI



Effective auditing therefore requires an inclusive understanding of stakeholders whose decisions, actions, or omissions affect DPI outcomes.

Table 4: Mapping Stakeholder Groups with Audit Concerns

Stakeholder Group	Roles & Responsibilities	Audit Interest
Government Entities/ Implementing Agencies	Policy formulation, funding, implementation and system oversight	Accountability, efficiency, value for money, compliance with inclusion and safety safeguards
Regulators and Data Protection Authorities	Oversight on data privacy, cybersecurity, competition, and access	Compliance with laws, ethical data use, and rights protection
Private Vendors/ System Integrators	Technology development, hosting, technical support	Contract compliance, cybersecurity assurance, system performance, and adherence to open standards

Stakeholder Group	Roles & Responsibilities	Audit Interest
Citizens and End-Users	Beneficiaries and contributors of data	Accessibility, informed consent, redressal mechanisms, and digital trust

This inclusive view aligns with ISSAI 3000's “Intended Users and Responsible Parties” paragraphs 25-28 and the UN Universal DPI Safeguards Framework's principle of multi-actor accountability: auditors must engage each responsible authority and stakeholder group to ensure that audit findings remain relevant, actionable, and oriented towards public value.

3.5 Mapping of Scope to People–Process–Tools & Technology and Data Governance

This section establishes the operational link between audit scope, audit objectives, and audit methodology through the People, Process, Tools & Technology and Data Governance lens. All subsequent audit planning, risk assessment, and evidence-gathering activities are expected to be aligned with this mapping. This multi-dimensional approach reflects the UN Universal DPI Safeguards Framework (2024), which emphasises responsible authorities, lifecycle stages, and safeguards for inclusion, safety, and sustainability across all DPI operations.

The standards and frameworks cited below function as reference audit criteria for evaluating controls, safeguards, and governance arrangements within each People, Process, Tools & Technology and Data Governance dimension.

Table 5: Mapping PPT&D Audit Dimension to the Reference Standards/ Audit Criteria

Audit Dimension	Example in DPI Context	Reference Standards/ Audit Criteria
People	Governance boards, IT staff, vendors, regulators, and citizens as users and data subjects	ISSAI 100 Fundamental Principles; ISSAI 130 (Ethics); ISSAI 3000 Performance Audit; GUID 5280 Audit of Public Procurement; ISO 10019 (Competence Management); Applicable public service rules and conduct regulations; UN DPI Safeguards – Responsible Authorities; ISO/ IEC 38500 IT Governance; ISO 9241 Human-Centred Design; ISO/ IEC 23894 AI Risk Management; WCAG 2.1 Web Accessibility; UN CRPD Rights of Persons with Disabilities.
Process	Procurement, grievance redress, change management	ISSAI 100; ISSAI 3000; ISSAI 4000 Compliance Audit; GUID 5100 Audit of Information Systems; GUID 5280; ISO 9001 (Quality Management); National procurement rules and financial regulations; Sectoral service delivery guidelines; UN DPI Safeguards Lifecycle Stages; UNCITRAL Model Law on Procurement; UN CRPD Rights of Persons with Disabilities.

Audit Dimension	Example in DPI Context	Reference Standards/ Audit Criteria
Tools & Technology	Platforms, APIs, registries, authentication systems	ISO/ IEC 38500 IT Governance; ISO 22301 a Business Continuity; OECD Data Governance/ AI Principles; GDPR/ National Data Protection Laws; ISSAI 100; ISSAI 3000; ISSAI 4000; ISSAI 5100; ISSAI 5101; ISO 27001 (Information Security); National cybersecurity policies and IT standards; Sectoral technology regulations; UN DPI Safeguards – Safety and Trust Principles; ISO 22301 a Business Continuity; ISO 9241; ISO 27040 Storage Security; ISO/ IEC 23894; WCAG 2.1; OECD Data Governance/ AI Principles; W3C/ ITU Interoperability Standards.
Data Governance Lifecycle	Data creation, sharing, retention, archival, deletion	ISSAI 100; ISSAI 3000; ISSAI 4000; GUID 5100; ISO 15489 (Records Management); ISO 8000 Data Quality; ISO 27040; ISO 27701 (Privacy Information Management); Applicable data protection and records management laws; OECD Data Governance Framework/ AI Principles; UN DPI Safeguards – Inclusion and Structural Integrity Principles; GDPR/ National Data Protection Laws.

By explicitly mapping every audit activity to these dimensions, SAIs can ensure complete and balanced coverage, capturing technical performance, institutional accountability, and data ethics within a unified framework.

This integration also enables seamless alignment between these Guidelines and the Audit Design Matrix (ADM), ensuring that each audit question is traceable to a responsible actor (People), governance or operational process (Process), technology or platform (Tools & Technology), and stage in the data lifecycle (Data Governance).

By applying this mapping systematically, auditors can ensure that no material governance, technical, or data-related risk remains outside audit coverage. This approach prevents fragmented analysis by integrating institutional accountability, operational controls, technological architecture, and data lifecycle management within a single, coherent audit structure. In applying these Guidelines, auditors shall give primary consideration to applicable national laws and sector-specific regulations, using international standards as complementary benchmarks.

3.6 Audit Mandate, Jurisdiction and Period

The extent, depth, and methods of DPI auditing are shaped by each Supreme Audit Institution's constitutional and legal mandate.

Audit **jurisdiction** should encompass all entities exercising fiduciary, technical, or custodial control over DPI assets, including implementing ministries, nodal agencies, regulators, shared platforms, and data custodians. This prevents audits from being confined narrowly to a single implementing entity while material governance or operational risks reside elsewhere in the ecosystem.

Where SAIs do not have direct authority over private-sector vendors or service providers, assurance may be obtained indirectly through:

- examination of contract provisions and procurement frameworks;
- review of service-level agreements, performance reports, and incident logs;
- reliance on third-party certifications, independent audits, or regulator reports; and
- verification of oversight mechanisms exercised by the audited public entity.

Consistent with the UN Universal DPI Safeguards Framework's recognition of shared responsibility among policy, implementing, and oversight authorities, SAIs are encouraged to recommend that future DPI contracts include explicit audit and access-to-information clauses, enabling review of critical vendor data, algorithmic transparency, and performance metrics in the public interest.

The **audit period** should be determined based on the lifecycle maturity of the DPI system, whether it is in design, rollout, scaling, or operational phase. Jurisdictional coverage should include all entities exercising fiduciary, technical, or custodial control over DPI assets. This ensures that the audit does not remain limited to the implementing ministry but extends to associated agencies, regulators, and partners holding relevant data or governance responsibilities. Audits may therefore span multiple years or phases to capture systemic risks, path dependencies, and cumulative impacts rather than isolated point-in-time performance.

In planning audit coverage, SAIs should assess whether collaborative and ecosystem-based arrangements are auditable in practice, considering:

- **Mandate** – clarity of legal authority to audit multi-actor DPI ecosystems, including private vendors and shared platforms;
- **Technology** – availability and reliability of system logs, audit trails, APIs, and data access necessary for verification; and
- **Risk Factors** – materiality and exposure arising from governance, inclusion, data governance, procurement, cybersecurity, or ethical risks.

These considerations help determine the depth, scope, and feasibility of audit work on collaboration and ecosystem governance in DPI.

Where reliance is placed on third-party certifications (such as ISO/IEC 27001, PCI DSS, SWIFT Customer Security Programme, or assessments under the Principles for Financial Market Infrastructures), auditors should evaluate: (a) the independence and accreditation of the certification body; (b) the scope and coverage of the certification relative to the audit objectives; (c) the recency of the certification and whether material changes have occurred since issuance; and (d) whether residual risks or control gaps identified in the certification report require supplemental audit procedures. Reliance should be documented and proportionate to the assurance provided.

3.7 Summary of Key points

- **Purpose of DPI audits** is to assess whether digital public infrastructure systems are designed, implemented, and operated in a manner that ensures **inclusion, equity, transparency, accountability, privacy, and security**.
- DPI audits evaluate whether **governance structures, operational controls, and data-management practices** comply with legal, ethical, and international standards throughout the **entire data lifecycle**.
- **Audit scope extends beyond individual applications** to the entire DPI ecosystem, including legislation, governance frameworks, architecture, operational processes, and sectoral implementations.
- DPI ecosystems involve **multiple stakeholders**, including government agencies, regulators, private vendors, and citizens; audits must therefore evaluate accountability across all actors.
- Audit mandates should cover **all entities exercising fiduciary, technical, or custodial control over DPI systems**, including public agencies, shared platforms, and private vendors where possible.

An abstract graphic of a network or mesh structure, composed of numerous small blue dots connected by thin lines, forming a complex, interconnected web that spans the lower half of the page.

CHAPTER-4

INTERNATIONAL STANDARDS AND FRAMEWORKS

CHAPTER-4

INTERNATIONAL STANDARDS AND FRAMEWORKS

The international standards and frameworks presented in this section serve as authoritative sources of audit criteria that support the application of the People, Process, Tools & Technology, and Data Governance (PPT&D) framework. They do not constitute independent analytical models for DPI audits. Instead, they provide benchmarks, control objectives, and normative references that enable auditors to assess each PPT&D dimension consistently and objectively.

Auditors should therefore apply these standards in an integrated manner, mapping relevant provisions to:

- Institutional roles (People),
- Governance mechanisms (Process),
- System architecture and controls (Tools & Technology), and
- Data lifecycle management practices (Data Governance).

The international standards and frameworks described in this chapter (ISSAI, ISO, OECD, GDPR, *etc.*) should be applied in conjunction with the UN Framework's principles of inclusion, safety, and structural integrity, ensuring that DPI audits remain consistent with both professional auditing standards and global digital-governance safeguards.

The frameworks listed in this section represent internationally recognised primary audit criteria. However, SAIs operate within diverse legal and institutional environments, and auditors may draw on alternative or complementary audit criteria where these are more specific, legally mandated, or contextually appropriate. Such criteria may include national laws and regulations governing data protection, digital identity, payments, or cybersecurity; regional regulatory frameworks; and recognised good practices established by SAIs or competent national authorities. Where alternative criteria are used, auditors should document the basis for their selection, ensure that the criteria are suitable, relevant, and reliable in accordance with ISSAI 3000 paragraph 45, and cross-reference them to the relevant PPT&D dimension and risk category.

The standards and frameworks described in this chapter (ISSAI, ISO, OECD, GDPR, *etc.*) should be applied in conjunction with the UN Framework's principles of inclusion, safety, and structural integrity to ensure that DPI audits remain consistent with both professional auditing standards and global digital-governance safeguards. A quick reference of standards mapped to PPT&D dimensions is provided in **Annexure D**. Standards with cross-cutting applicability (*e.g.*, ISSAI 100 and the UN Universal DPI Safeguards Framework) apply across all dimensions and serve as overarching audit authorities. Detailed guidance on each standard is provided in **Paragraphs 4.1 through 4.8**.

4.1 INTOSAI Framework: Foundational Principles and Standards

The *International Standards of Supreme Audit Institutions (ISSAIs)* provide the universal foundation for public-sector auditing. These Guidelines for auditing Digital Public

Infrastructure (DPI) derive their authority and structure from the **INTOSAI Framework of Professional Pronouncements (IFPP)**.

Key references include:

- **ISSAI 100 – *Fundamental Principles of Public-Sector Auditing***: establishes the purpose of public-sector audits to strengthen accountability, transparency, and good governance.
- **ISSAI 130 – *Code of Ethics***: underlines integrity, independence, and competence as the bedrock for audits involving high public interest and sensitive data.
- **ISSAI 3000 – *Performance Audit Standard***: provides requirements for planning, conducting, and reporting on audits of efficiency, economy, and effectiveness.
- **ISSAI 4000 – *Compliance Audit Standard***: defines the framework for assessing conformity with laws, regulations, and authorities, essential when auditing digital systems and data practices.

DPI audits embody elements of both **performance** (effectiveness, inclusion, efficiency) and **compliance** (security, privacy, accessibility) auditing. SAIs should therefore apply these standards in a complementary manner.

4.2 INTOSAI Guidance on Thematic Areas

Certain INTOSAI Guidance (GUID) documents directly address topics relevant to DPI audits:

- **GUID 5100 – Guidance on Audit of Information Systems**: Defines how auditors should assess IT controls, data reliability, system integrity, and cybersecurity. It emphasises evaluating both *general controls* (governance, security, continuity) and *application controls* (input, processing, output). In DPI contexts, auditors should use this GUID when examining APIs, registries, payment systems, and data exchanges.
- **GUID 5101 – Guidance on Information Security Audits**: provides detailed criteria for assessing information-security governance, risk management, and control effectiveness, complementing GUID 5100.
- **GUID 5280 – Guidance on Audits of Public Procurement**: Relevant for DPI implementation, which typically involves complex procurement of IT hardware, software, and managed services. Auditors should examine whether procurement processes are transparent, competitive, and aligned with open-standards principles to prevent vendor lock-in and ensure sustainability.
- **GUID 3910 (Central Concepts for Performance Auditing) and GUID 3920 (The Performance Auditing Process)** for detailed process-level guidance. Together, GUID 5100 and 5280 operationalize ISSAI 3000's general requirements on *skills, communication, and audit criteria* by providing practical audit points for IT governance and procurement.

4.3 ISO Standards: Security, Privacy, Continuity and Accessibility

The International Organization for Standardisation (ISO) complements ISSAI requirements through domain-specific controls that can be used as **audit criteria**:

Table 6: Relevant Standards mapped to Audit Domains

Domain	Relevant Standards	Audit Relevance
Information Security	ISO/ IEC 27001 and 27002	Establish frameworks for managing information security and defining controls for confidentiality, integrity, and availability.
IT Governance	ISO/ IEC 38500	Provides a governance framework for corporate oversight of IT, covering responsibility, strategy, acquisition, performance, conformance, and human behaviour. Relevant for assessing whether DPI governing bodies exercise appropriate oversight under the People and Process dimensions.
Privacy Management	ISO/ IEC 27701	Extends ISO 27001 to incorporate data-protection principles consistent with GDPR; critical for DPI audits covering personal data.
Business Continuity	ISO 22301	Provides methods for resilience, redundancy, and disaster recovery of digital systems which are core to service continuity in DPI.
Accessibility and Usability	ISO 9241-210, WCAG 2.1	Ensures DPI systems are inclusive for users with varying abilities and access conditions.
Data Quality	ISO 8000	Defines standards for data accuracy, completeness, and consistency, essential for high-integrity registries and transactions.
Records Management and Storage Security	ISO 15489, ISO 27040	Establish retention, archival, and disposal protocols crucial for the Data Governance Lifecycle component of DPI audits.

When citing these standards, auditors should assess how well national laws and organisational policies align with them rather than expecting full certification conformity.

4.4 Data Protection and Privacy Frameworks

The **General Data Protection Regulation (GDPR)** and comparable national frameworks (such as *India's Digital Personal Data Protection Act, 2023*) articulate rights and obligations around personal data processing. These principles *i.e.* lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and accountability are globally recognised.

For DPI audits, SAIs should examine whether:

- Citizens are informed about data collection and consent processes;
- Data use aligns with stated purposes;
- Retention and deletion policies are explicit and enforced; and
- Oversight institutions (*e.g.*, Data Protection Authorities) function independently and effectively.

Such criteria correspond to ISSAI 3000's requirement for suitable audit criteria (para. 45) and ISSAI 4000's emphasis on legal and regulatory compliance. These principles are also reflected in the UN Universal DPI Safeguards Framework (2024), which identifies privacy and data protection as central to its 'Risks to Safety' dimension.

4.5 Open Data, Interoperability, and Competition

Audit of DPI must also verify compliance with principles of openness and fair competition. References include:

- **OECD Open Government Data Charter** – promotes transparency, reuse, and innovation through open data.
- **W3C and ITU standards** – define interoperability and web-accessibility protocols that ensure inclusivity and vendor neutrality.
- **OECD Competition Principles and UNCITRAL Model Law on Public Procurement** – ensure fair contracting, prevent monopolistic behavior, and encourage market-based innovation.

Evaluating these principles enables auditors to test whether DPI platforms create public value without distorting markets or restricting future innovation, a key concern noted in both *GUID 5280* and the *DPI ADM* Matrix included in the document.

4.6 AI and Algorithmic Governance Standards

As DPI systems increasingly incorporate automated decision-making, algorithmic processing, and AI-assisted service delivery, auditors must apply appropriate criteria to evaluate the governance, transparency, and accountability of these components.

The key reference standards for this domain are:

- **ISO/ IEC 23894:2023 – Guidance on Risk Management for AI:** provides a structured framework for identifying, assessing, and treating risks specific to AI systems, including risks of bias, opacity, unintended behaviour, and failure of human oversight. This is the primary technical audit criterion for evaluating AI risk governance in DPI contexts. Auditors should use it when examining whether AI components within DPI have undergone appropriate risk assessment, whether controls are in place to detect and correct bias, and whether accountability for automated decisions is clearly assigned.
- **OECD Principles on AI (2019, updated 2024):** provide policy-level criteria on Transparency, Explainability, Human Oversight, Accountability, and Robustness of AI systems. These are particularly relevant for assessing whether the governance framework surrounding DPI's AI components aligns with internationally recognised norms.
- **OECD AI Policy Observatory** guidance documents on algorithmic accountability and public-sector AI deployment complement these principles for SAI use.

Both ISO/ IEC 23894 and the OECD AI Principles serve as audit criteria under the Tools & Technology and People PPT&D dimensions respectively; the former for technical AI risk controls, the latter for governance and human oversight arrangements. Design Risks associated with algorithmic bias, opacity, and exclusionary interfaces (as defined in **Paragraph 5.4**) should be assessed against these criteria.

4.7 Accessibility and Inclusion Standards

Accessibility and inclusion underpin the purpose of DPI. Auditors should verify whether platforms comply with the **Web Content Accessibility Guidelines (WCAG 2.1)**, **ISO 9241**, and national accessibility legislation (where applicable). This ensures services are usable by all citizens, including persons with disabilities, older populations, and those in low-connectivity environments. ISSAI 3000's focus on *effectiveness* and *equity* aligns directly with this criterion.

4.8 Data Governance and Lifecycle Standards (Generic Framework)

To maintain global neutrality, this document adopts a *generic Data Governance Lifecycle* framework consistent with international standards rather than any single national policy. Auditors should assess DPI data management across six phases:

1. **Creation and Collection** – legality, proportionality, and informed consent.
2. **Use and Processing** – adherence to stated purposes and role-based access.
3. **Sharing and Disclosure** – interoperability, contractual safeguards, cross-border data flow compliance.
4. **Storage and Retention** – secure, redundant, and duration-bound storage per ISO 27040 and 22301.
5. **Archival and Preservation** – long-term integrity and retrievability per ISO 15489.
6. **Deletion and Disposal** – irreversible erasure, audit trails of deletion, compliance with retention schedules. These phases correspond directly to audit evidence expectations in ISSAI 3000 (paragraphs 35-49). Each can be associated with a distinct audit question in the ADM, linking technical control to governance accountability. This lifecycle view aligns with the UN DPI Safeguards Framework's emphasis on continuous accountability and risk mitigation across its five stages: **Conception and Scoping, Strategy and Design, Development, Deployment, and Operations and Maintenance** while recognising that a final **decommissioning phase**, though not explicitly defined in the Framework, remains essential for ensuring secure data disposal and system closure.

4.9 National and Regional Adaptations

While the standards above offer universal guidance, each SAI should adapt them to its legal and institutional context. Examples include:

- *India's Data Governance Framework and Digital Personal Data Protection Act;*
- *EU Data Governance Act and eIDAS Regulation;*
- *Singapore's Model AI Governance Framework; and*
- *African Union Digital Transformation Strategy (2020–2030).*

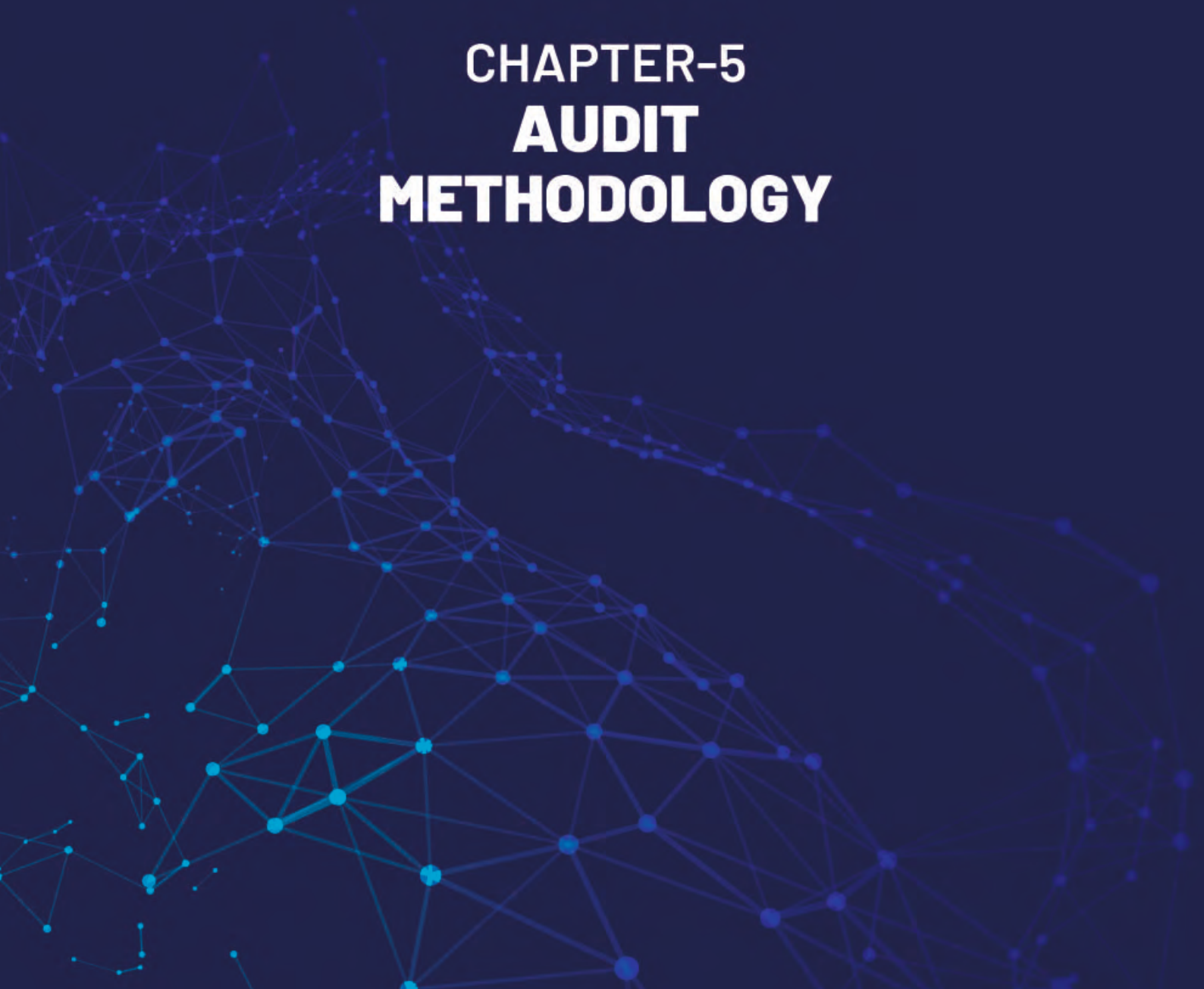
Such cross-references allow SAIs to benchmark national frameworks without compromising neutrality.

SAIs may also draw on supplementary IT governance and assurance frameworks commonly used in their institutional contexts. COBIT 2019 (Control Objectives for Information and Related Technologies, maintained by ISACA) is an integrated IT governance, management, and assurance framework that originated as a set of IT audit control objectives and continues to incorporate assurance components through ISACA's IT Assurance Framework (ITAF). ITIL 4 (Information Technology Infrastructure Library) is a widely adopted best-practice framework for IT service management covering service design, transition, operations, and continual improvement, and while not an audit standard, it provides a useful reference for assessing structured practices such as service continuity, incident management, change control, and service-level monitoring.

COBIT's control objectives for IT governance, risk management, and service delivery may serve as complementary reference criteria alongside GUID 5100 and relevant ISO standards, while ITIL concepts may be used as a supplementary lens when evaluating the Process and Tools & Technology dimensions of DPI governance, where applicable in their jurisdictional context. SAIs may refer to the INTOSAI WGITA Cybersecurity and Data Protection Audit Guidelines, if within the validity, which details appropriately the reference of NIST CSF too.

4.10 Summary of Key points

- **International standards** (ISSAI, ISO, OECD, GDPR, *etc.*) provide audit criteria to evaluate DPI systems and serve as **benchmarks and control references** to assess governance, technology, and data practices objectively.
- **Data protection frameworks** such as GDPR and national laws establish principles for lawful data processing, including **consent, purpose limitation, data minimisation, retention limits, and accountability**.
- **AI governance standards** such as **ISO/ IEC 23894** and **OECD AI Principles** provide criteria to audit algorithmic decision-making, focusing on **risk management, transparency, human oversight, and bias mitigation**.
- **Accessibility and inclusion standards** (WCAG 2.1 and ISO 9241) ensure digital services are usable by **persons with disabilities and citizens with varying digital access conditions**.
- Additional **IT governance and service management frameworks** to GUID 5100 & 5101 for IT systems and information security audits such as **COBIT and ITIL** can support DPI audits by providing guidance on **IT governance, risk management, service delivery, and operational controls**.

An abstract graphic in the bottom-left corner of the page, consisting of a complex network of interconnected nodes and lines. The nodes are represented by small circles in various shades of blue and teal, while the lines are thin and light blue. The network forms a dense, organic shape that extends from the bottom-left towards the center of the page.

CHAPTER-5

AUDIT METHODOLOGY

CHAPTER-5

AUDIT METHODOLOGY

5.1 Integrated Audit Approach

Comprehensive auditing of DPI requires a **hybrid methodology** that integrates three audit perspectives defined within the INTOSAI framework:

- **Performance Audit** (ISSAI 3000): evaluates *economy, efficiency, and effectiveness* of DPI systems in achieving inclusion, accessibility, and service outcomes.
- **Compliance Audit** (ISSAI 4000): verifies conformity with applicable laws, data-protection regulations, procurement rules, and accessibility standards.
- **Information Systems Audit** (GUID 5100): examines technical controls, cybersecurity, data integrity, and continuity mechanisms underpinning DPI platforms.

A DPI audit should blend these lenses seamlessly, recognising that performance outcomes often depend on compliance and technical integrity. Accordingly, the risk areas identified through the DPI risk assessment namely **inclusion risks, design risks, data governance risks, operational risks, and accountability risks** should determine the audit focus and guide the selection of the most appropriate audit perspective.

Each audit engagement should therefore define:

1. **Primary audit type** (performance, compliance, or hybrid),
2. **Level of assurance** expected, and
3. **Scope of IT testing** required.

The choice of primary audit approach should be determined by the SAI's mandate, the governing legal framework, and the primary audit question guiding the engagement. Where the central question concerns policy outcomes, inclusion, or value for money, the audit will typically be performance-oriented; where legality, regulatory compliance, or contractual obligations are central, a compliance approach may be more appropriate. In many DPI engagements, however, both dimensions are relevant, and a hybrid approach is applied in which compliance establishes the legal and regulatory baseline while performance analysis evaluates whether that baseline delivers intended public value. Where technical controls, cybersecurity, data integrity, or system resilience are material to the audit objectives, information systems audit procedures consistent with GUID 5100 should be incorporated within the engagement.

5.2 Planning and Scoping

Per ISSAI 3000 (paragraphs 23-24), planning should begin with **topic selection** based on materiality, risk, and relevance to public interest. For DPI, this includes:

- *Materiality*: number of users affected, financial scale, and strategic importance;
- *Risk*: likelihood of systemic exclusion, data misuse, or vendor dependency;

- *Relevance*: national priorities on inclusion, privacy, or digital rights. Auditors should prepare a **Planning Memorandum** documenting:
 - Audit objectives and sub-objectives (as per Chapter 6),
 - Expected outcomes,
 - Resource plan and skill mix,
 - Applicable standards and criteria (cross-referenced to Chapter 4), and
 - Stakeholder map (responsible entities, intended users, partners).

A preliminary risk scan using open data, prior audit reports, and grievance statistics helps refine scope and focus areas.

5.3 Data Collection and Evidence Techniques

Consistent with ISSAI 3000 (paragraphs 38-49) and GUID 5100, audit evidence for DPI must combine **documentary**, **technical**, and **stakeholder-based** inputs.

Typical methods include:

- **Document Review** – policies, architecture documents, contracts, DPI usage analytics.
- **Data Extraction and Transaction Analysis (where permissible)** – obtaining transaction-level or system-generated data to perform analytical testing, trend analysis, or anomaly detection. Such data-driven procedures help auditors obtain direct assurance on completeness, accuracy, and integrity of DPI operations, in compliance with applicable privacy and confidentiality provisions.
- **System Examination** – walkthroughs, configuration reviews, programming logic/ source-code sampling (where permissible) - examining selected portions of program logic or scripts to verify whether critical application controls, security routines, or data-validation mechanisms are correctly implemented. Source-code sampling is performed on a *risk-based* basis and only with authorised access to protect intellectual property and confidentiality. It provides assurance that system behaviour aligns with documented specifications and control requirements, followed by API testing, and log analysis.
- **Interviews and Focus Groups** – with citizens, developers, regulators, and grievance officers to assess inclusion and accessibility.
- **Surveys / User Testing** – capturing feedback from vulnerable groups on usability and access barriers.
- **Analytical Procedures** – analysing transaction logs for anomalies, downtime, or data-quality issues (ISO 8000).

Auditors should apply the People, Process, Tools & Technology and Data Governance lens to evidence-gathering:

- *People*: capacity and competence of implementing staff;
- *Process*: adequacy of controls and documentation;
- *Tools & Technology*: configuration and functionality checks;
- *Data*: lifecycle compliance and privacy-by-design indicators. All evidence should be **triangulated** to ensure reliability, as required by ISSAI 3000 paragraph 33 (“assurance

through transparent communication of methodology and data collected”). Significant findings should therefore be supported by multiple independent evidence sources. Where evidence sources conflict, auditors should obtain additional evidence where feasible or transparently disclose the limitations.

5.4 Risk Assessment Framework

Digital Public Infrastructure (DPI) comprises technological systems and services that operate at the intersection of individuals, on the one hand, and civic, public, and private actors that exercise social, political, and economic power, on the other. As a result, risks associated with DPI do not arise solely from technical weaknesses but also from deficiencies in design choices, data governance practices, operational arrangements, and accountability structures, as well as from broader normative (ethical, legal, and regulatory) and institutional constraints.

Auditors must actively manage audit risk *i.e.* the risk of reaching incorrect or incomplete conclusions throughout the audit engagement (ISSAI 3000, paragraph 52). In the context of DPI, risk assessment should therefore extend beyond conventional system and compliance risks to include **digital-ecosystem-specific and rights-relevant dimensions**. The DPI risk matrix should be structured around the following core risk categories:

Table 7: DPI Risk Categories for Audit Planning

Risk Category	Description	Illustrative Indicators	Related Standards/ Frameworks
Inclusion Risk	Unequal access, exclusion, or disempowerment of individuals or groups due to socio-economic, geographic, linguistic, or ability-related barriers	Limited coverage of remote or marginalised populations, absence of assisted access channels, lack of multilingual or accessibility features	WCAG 2.1, ISO 9241, UN DPI Safeguards – Risks to Inclusion (Access, Equity)
Design Risks	Harm arising from system or algorithmic design choices, including bias, opacity, or exclusionary interfaces	Automated decisions without explainability, inaccessible user interfaces, absence of human-in-the-loop controls	OECD AI Principles, ISO/ IEC 23894 (AI Risk Management); UN DPI Safeguards – Risks to Inclusion (Fairness, Explainability)
Data Governance Risks	Weaknesses in the management of the data lifecycle leading to privacy violations, surveillance, or loss of user agency	Inadequate consent mechanisms, excessive data retention, insecure or non-purpose-bound data sharing	ISO/ IEC 27701, ISO 15489, UN DPI Safeguards – Risks to Safety (Privacy, Data Integrity)

Risk Category	Description	Illustrative Indicators	Related Standards/ Frameworks
Operational Risks	Risks arising from system operation and ecosystem dependencies, including sustainability, resilience, and security concerns; absence of cloud exit strategy or data portability provisions, and insufficient internal operational capability to sustain DPI infrastructure independently of vendors	Vendor lock-in, absence of continuity and disaster recovery planning, cybersecurity incidents, single points of failure; no documented cloud exit or data portability plan, inability of internal teams to operate DPI infrastructure independently of vendors	ISO/ IEC 27001, ISO 22301, GUID 5280, ISO/ IEC 38500 (IT Governance), UN DPI Safeguards – Structural Vulnerabilities (Sustainability, Resilience)
Accountability Risks	Weak oversight, unclear ownership, or ineffective redress mechanisms across public–private actors; Fragmented governance structures and uncoordinated digital initiatives	Overlapping mandates, lack of grievance redressal mechanisms, monopoly control over critical DPI components; Fragmented governance acting as a driver of systemic failure and non-sustainability; Systemic vulnerabilities beyond any single system due to coordination failure	ISSAI 100, ISSAI 123 UN DPI Safeguards - Structural Vulnerabilities (Governance, Rule of Law, Non-sustainability)

In the DPI context, legal risk refers to the potential for legal disputes, regulatory non-compliance, or unenforceable accountability arising from the collection, use, management, and regulation of DPI systems and their data. This includes gaps in enabling legislation, ambiguity in liability between public and private DPI actors, jurisdictional uncertainties in cross-border data flows, and absence of legally enforceable rights for citizens affected by automated decisions.

Auditors should assess legal risk as an amplifying factor across each of the five categories – particularly where regulatory frameworks are nascent or where private-sector actors operate DPI components under inadequately defined legal mandates. Auditors should also recognise that many exclusion and accountability risks stem not only from technical design failures but from fragmented institutional mandates and uncoordinated digital initiatives across government agencies. A **Whole-of-Government lens** – as articulated in OECD guidance on whole-of-government approaches – is therefore essential at the scoping stage, enabling auditors to identify systemic causes of exclusion that span multiple agencies, budget lines, and policy frameworks rather than residing within any single DPI system.

Each identified risk should be assessed in terms of **impact and likelihood**, with explicit linkage to:

- relevant controls and safeguards,
- stages of the data lifecycle (creation → use → sharing → retention → deletion), and
- the roles and responsibilities of public and private actors within the DPI ecosystem.

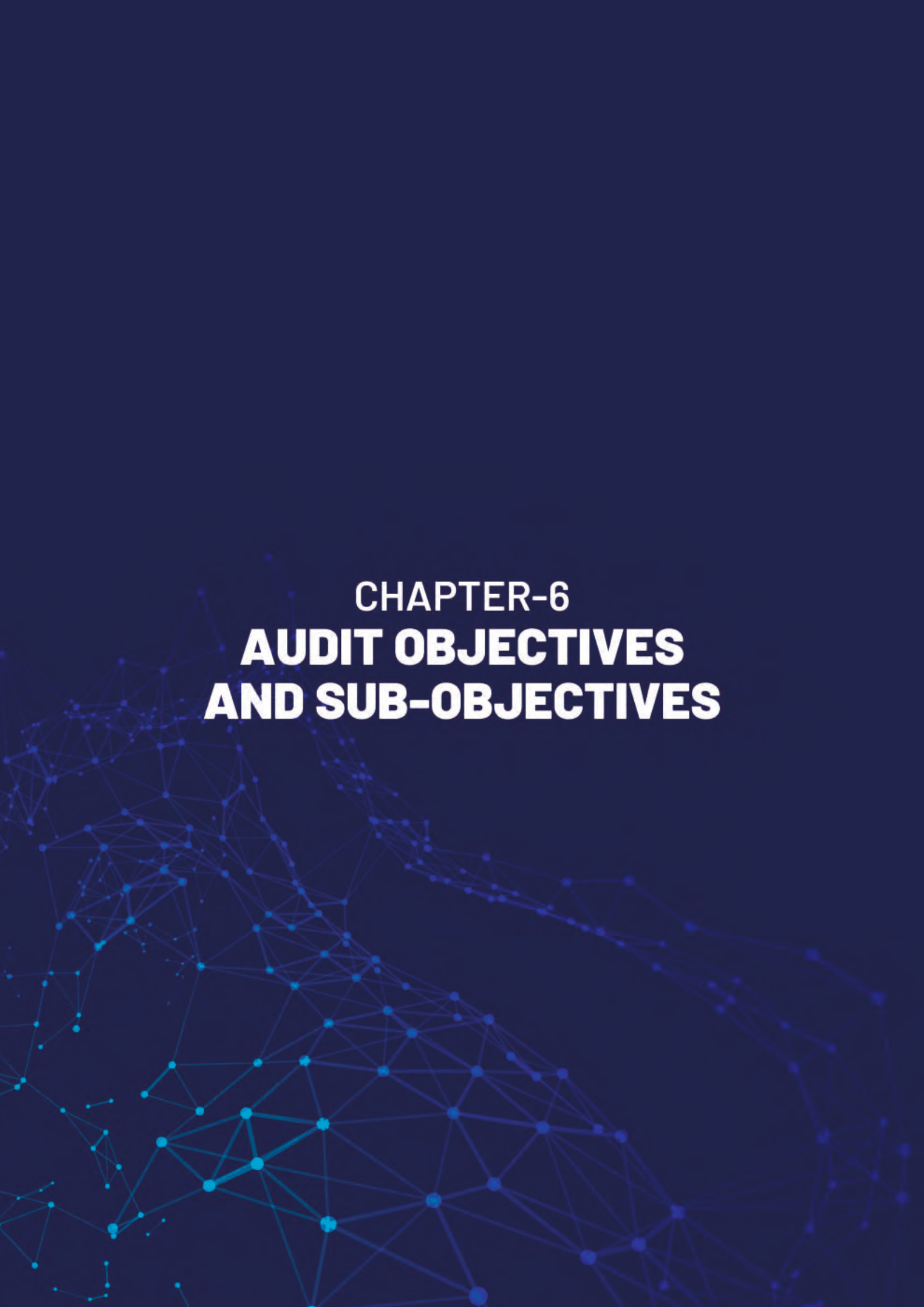
This structured risk assessment provides the basis for determining audit priorities, selecting appropriate audit criteria, and tailoring audit procedures to address both performance and rights-related dimensions of DPI.

When scoring for assessing impact and likelihood for each DPI risks, auditors should consider the following factors:

- *Impact* reflects the potential severity of harm if the risk materialises. For DPI risks, impact should be assessed across four dimensions:
 - (a) **scale** — how many citizens or transactions are affected;
 - (b) **rights severity** — whether the harm involves deprivation of access, privacy violation, or loss of remedy;
 - (c) **reversibility** — whether the harm can be corrected or is systemic and self-reinforcing; and
 - (d) **institutional consequence** — whether the failure undermines public trust, regulatory authority, or DPI sustainability.
- *Likelihood* reflects the probability that the risk will materialise given existing controls. Auditors should consider:
 - (a) **qualitative indicators** such as absence of policy, weak oversight, prior incidents or complaints, audit findings from prior cycles, and known technical vulnerabilities; and
 - (b) **quantitative indicators** where data are available, such as system downtime rates, exclusion or rejection rates in identity or payment systems, grievance volumes, percentage of population without DPI access, and API error rates. The combination of impact and likelihood should produce a **High/ Medium/ Low** severity rating which then drives the prioritisation of audit findings and the urgency of recommendations. In lower-maturity DPI environments where quantitative data may be limited, auditors should apply professional judgement and weigh qualitative indicators more heavily, documenting the basis for their assessment transparently in line with ISSAI 3000.

5.5 Summary of Key points

- **DPI audits require an integrated approach** combining three audit perspectives: **Performance Audit (ISSAI 3000)** – economy, efficiency, effectiveness, inclusion outcomes, **Compliance Audit (ISSAI 4000)** – adherence to laws, regulations, and standards and **Information Systems Audit (GUID 5100)** – technical controls, cybersecurity, and data integrity.
- Risk evaluation should consider both **impact and likelihood**, including factors such as scale of affected citizens, severity of rights impact, reversibility of harm, and institutional consequences.
- DPI audits should adopt a **Whole-of-Government perspective**, recognising that many risks arise from fragmented governance across multiple agencies rather than a single system.

An abstract graphic in the bottom-left corner of the page, consisting of a complex network of interconnected nodes and lines. The nodes are represented by small blue dots, and the lines are thin, light blue lines. The network forms a dense, irregular shape that tapers off towards the right, resembling a stylized map or a data visualization of a network.

CHAPTER-6

AUDIT OBJECTIVES AND SUB-OBJECTIVES

CHAPTER-6

AUDIT OBJECTIVES AND SUB-OBJECTIVES

6.1 Purpose of Defining Audit Objectives

In accordance with **ISSAI 3000 Paragraphs 35-37**, each DPI audit must articulate *clearly defined audit objectives* that specify what will be examined, why it matters, and how success will be assessed against established criteria.

The audit objectives set out below are structured and applied through the People-Process- Tools & Technology and Data Governance (PPT&D) Framework described in **Paragraphs 1.5 and 3.5**. These objectives reflect the UN Universal DPI Safeguards Framework (2024), which clusters risks and principles under three broad dimensions *i.e.* **inclusion, safety, and structural integrity** and follows accountability across five lifecycle stages: **Conception & Scoping, Strategy & Design, Development, Deployment, and Operations & Maintenance**.

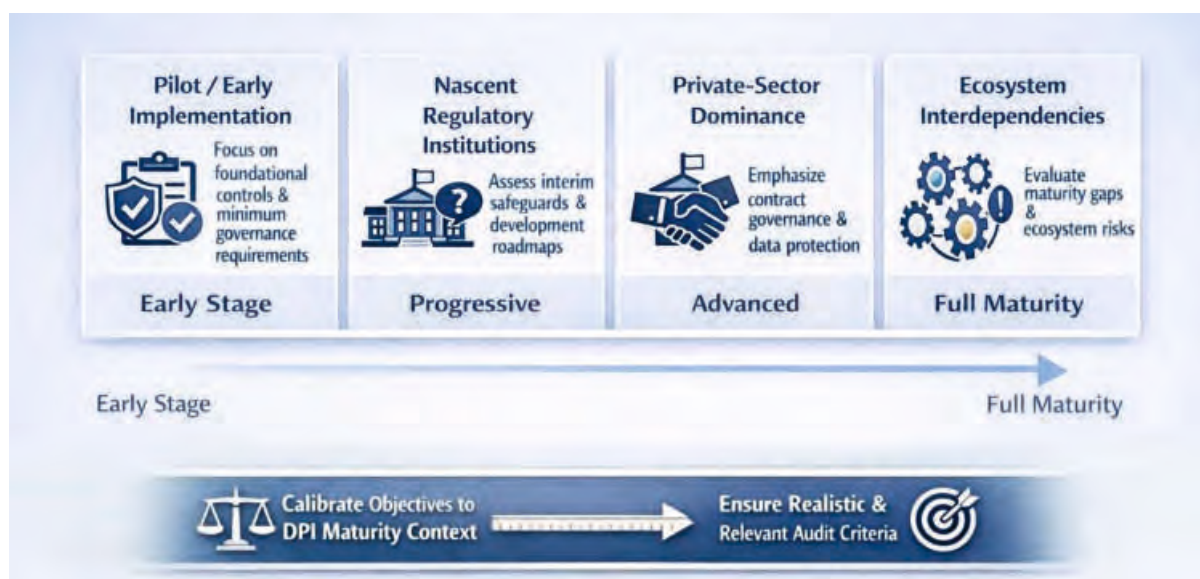
For the purposes of these Guidelines, the lifecycle assessment is extended to include decommissioning and archival to ensure accountability for system closure, data retention, and secure disposal. This extension is consistent with **Paragraph 3.3's** treatment of the DPI lifecycle and with ISO 15489 (Records Management) and ISO 27040 (Storage Security), which establish obligations relating to data retention and secure deletion beyond operational decommissioning. Accordingly, where a DPI system is in or approaching this stage, auditors should include decommissioning and archival considerations within the scope of the audit.

For Digital Public Infrastructure, the objectives are grouped into three inter-linked domains:

1. **Governance of DPI** – institutional arrangements, strategy, and control. (*structural integrity*)
2. **Engagement with Stakeholders** – participation, transparency, and accountability. (*inclusion + structural integrity*)
3. **Inclusion, Access & Privacy for Citizens** – fairness, accessibility, and protection of rights. (*inclusion + safety*)

These three objectives operationalise the audit purposes set out in **Paragraph 3.1**: assessing inclusive service delivery, governance and oversight arrangements, lawful and responsible data management, and the efficiency and sustainability of DPI outcomes, translating them into structured, testable domains aligned with the three dimensions of the UN Universal DPI Safeguards Framework.

Each objective connects to the People, Process, Tools & Technology and Data Governance lens and the relevant data lifecycle phase (*creation → use → retention → disposal*). In determining audit focus and refining objectives, auditors should consider DPI-related governance, inclusion, data governance, procurement and vendor, cybersecurity and operational, and ethical or AI-related risks, as these factors should guide the selection, prioritisation, and tailoring of audit objectives and sub-objectives across governance, stakeholder engagement, and citizen-centric dimensions of DPI.

Figure 8: Maturity-Based Adaptation of Audit Objectives

The audit objectives in this section presuppose a relatively developed DPI ecosystem with functioning regulatory institutions, established data protection authorities, and systems operating at or approaching scale. In practice, however, SAIs will encounter a wide spectrum of institutional and technological maturity. Auditors should therefore calibrate the application of audit objectives and criteria to the maturity of the DPI environment under review.

Different maturity contexts, such as early-stage implementation, evolving regulatory institutions, private-sector-led delivery models, or ecosystem interdependencies, require adjustments in audit focus. Rather than applying full operational performance benchmarks in all cases, auditors should prioritise foundational governance safeguards, institutional accountability arrangements, and mechanisms for managing ecosystem dependencies where these remain under development.

These adaptations do not reduce the rigour of the audit. Rather, they ensure that audit objectives and criteria remain proportionate to the institutional context and generate findings that are realistic and actionable, consistent with ISSAI 3000 paragraph 35 on the requirement that audit objectives be relevant and feasible.

The audit objectives and sub-objectives set out below are illustrative in nature. Auditors should identify and assess relevant risk factors specific to the DPI ecosystem under review and, where necessary, adapt or modify the Audit Design Matrix (ADM) to ensure that audit objectives, criteria, and procedures remain proportionate, risk-responsive, and context-specific.

6.2 Objective 1 – Governance of Digital Public Infrastructure

Audit Purpose:

To assess whether DPI initiatives are governed by robust, transparent, and accountable frameworks ensuring strategic alignment, resource efficiency, and data stewardship. This objective is examined through leadership capacity and accountability structures (People), governance and control mechanisms (Process), system architecture and security controls (Tools & Technology), and data stewardship arrangements (Data Governance).

Illustrative Broad Audit Questions

- How effectively does the overall governance structure of the DPI ensure accountability, transparency, and ethical integrity?
- Are institutional roles and decision-making authorities clearly defined and coordinated across ministries, regulators, and implementing agencies?
- Does the governance framework integrate privacy, security, and inclusion objectives into strategic planning and budgeting?

Are oversight mechanisms *i.e.* internal audit, external review, and citizen feedback functioning as intended?

Table 8: Sub-Objectives and Focus Areas for Objective 1 – Governance of DPI

Sub-Objective	Key Questions	PPT & D Focus	Reference Standards
6.2.1 Institutional Roles & Structures	Are governance roles and mandates clearly defined? Are oversight committees functional and independent? Do members of the DPI oversight or governance body possess demonstrable expertise in IT governance, IT risk management, information security, or program/ portfolio management?	<i>People</i> – clarity of responsibility and skills	ISSA 100; 130; GUID 5100 (IT Governance); ISO/ IEC 38500
6.2.2 Policies & Documentation	Are policies consistent with national strategies and international norms on openness, privacy, and interoperability?	<i>Process</i> – policy framework lifecycle	ISSAI 3000 Paragraph 45; ISO 27701; OECD Data Governance Principles
6.2.3 Human Resources & Skills	Do implementing entities possess technical, ethical, and managerial competencies to run DPI?	<i>People</i> capacity building	– ISSAI Paragraphs 63-65 3 IDI Capacity 3000; Development Framework
6.2.4 Budgeting & Delegation	Are budgeting and authorisation procedures transparent and performance-linked?	<i>Process</i> – financial control	ISSAI 4000 Paragraph 33; GUID 5280-4 (Financial controls)

6.2.5 Technology Management	Are technology choices guided by open standards, interoperability, and resilience principles and automated decision systems subject to bias testing, explainability requirements, and human oversight mechanisms?	<i>Tools & Technology</i> – architecture & security	GUID 5100 (General Controls); ISO 27001 & 22301; OECD AI Principles
6.2.6 Monitoring & Evaluation	Are KPIs and SLAs established and periodically reviewed?	<i>Process and Data</i> – performance logs, data quality	ISSAI 3000 Paragraphs 28–32; ISO 8000 (Data quality)

Data Lifecycle Emphasis: Alignment of data ownership, classification, retention, and archival controls across the Strategy & Design to Operations & Maintenance stages.

6.3 Objective 2 – Engagement with Stakeholders

Audit Purpose:

To determine whether DPI systems ensure effective collaboration among government entities, private partners, and citizens, under transparent and equitable arrangements. This objective is examined through stakeholder competencies and responsibilities (People), contracting and coordination arrangements (Process), interoperability and platform governance mechanisms (Tools & Technology), and consent and data-sharing controls (Data Governance).

Illustrative Broad Audit Questions

- How inclusive and transparent are stakeholder-engagement processes across the DPI ecosystem (government, vendors, citizens)?
- Do contracting and data-sharing arrangements safeguard public interest while encouraging innovation and competition?
- Are grievance redressal mechanisms, performance monitoring, and feedback loops effectively capturing and acting on user concerns?
- Is there evidence that collaboration and interoperability reduce duplication and enhance service quality?

Table 9: Sub-Objectives and Focus Areas for Objective 2 – Engagement with Stakeholders

Sub-Objective	Key Questions	PPT&D Focus	Reference Standards
6.3.1 Registration and Onboarding	Are registration and onboarding processes inclusive, secure, and verifiable?	<i>Process and Data</i> – identity proofing & verification	GUID 5100; ISO 27701 (Consent records)
6.3.2 Discovery and Access Mechanisms	Are DPI services discoverable and accessible through open APIs and catalogues?	<i>Tools & Technology</i> – API standards & documentation	W3C/ITU Interoperability Guidelines
6.3.3 Digital Rights & IP Management	Are data-sharing agreements OECD clauses fair and transparent?	<i>Process + People</i> – contract governance	GUID 5280; IPR Guidelines
6.3.4 Business Intelligence & Analytics	Is data analytics used responsibly to improve performance without violating privacy?	<i>Tools & Technology and Data</i> – AI ethics controls	OECD AI Principles; ISSAI 3000 Paragraph 45
6.3.5 Migration GUID	Are legacy systems with data integrity checks?	<i>Process and Tools</i> data conversion logs	ISO 27040;
6.3.6 Competition and Performance Management	Are vendor contracts performance-linked and non-exclusive?	<i>Process</i> – contract monitoring	GUID 5280; UNCITRAL Model Law
6.3.7 Grievance Redressal Mechanisms	Are user grievances captured, resolved, and analysed for systemic improvement?	<i>People and Process</i> – feedback loops	ISSAI 3000 Paragraph 58; ISO 10002 (Customer satisfaction)
6.3.8 Contract Management & Transparency	Do contract clauses enable audit rights and data portability?	<i>Tools and Process</i> – contract repositories	GUID 5280-7; ISSAI 4000 (Transparency)

Data Lifecycle Emphasis: Consent, sharing, portability, and third-party disclosure spanning the Development → Deployment → Operations stages.

6.4 Objective 3 – Inclusion, Access & Privacy for Citizens

Audit Purpose:

To verify whether DPI ensures equitable access for all users, protects personal data, and upholds citizens' digital rights through lawful, ethical, and user-centric design. This objective is examined through citizen awareness and digital literacy (People), access and redress mechanisms (Process), usability and security features (Tools & Technology), and privacy and lifecycle data protection safeguards (Data Governance).

This objective is directly anchored to the UN SDGs' **Leave No One Behind** principle, which requires that digital transformation actively reaches and empowers the most vulnerable and marginalised populations, including persons with disabilities, women and girls, elderly citizens, low-income groups, and those in remote or low-connectivity areas, rather than defaulting to outcomes that serve only those already advantaged.

Illustrative Broad Audit Questions

- Does the DPI design and operation ensure equitable access for all demographic and ability groups?
- Are privacy-by-design and consent-management principles implemented throughout the data lifecycle?
- How effectively do digital-literacy and communication strategies enable citizens to use and trust DPI services?
- Are data-protection, security, and redress mechanisms aligned with international best practices and national laws?

Table 10: Sub-Objectives and Focus Areas for Objective 3 – Inclusion, Access & Privacy for Citizens

Sub-Objective	Key Questions	PPT&D Focus	Reference Standards
6.4.1 Information, Education & Communication	Are citizens adequately informed about DPI services, risks, and rights?	<i>People and Process</i> – awareness outreach	ISSAI 100 (Public value); UN CRPD & Art. 9
6.4.2 Registration with Minimal Data	Is only essential data collected? Are alternate ID options available?	<i>Data</i> – minimisation principle	GDPR Art. 5(1)(c); ISO 27701-7.4
6.4.3 User Experience & Accessibility	Are interfaces compliant with WCAG 2.1 and ISO 9241 standards?	<i>Tools & Technology and People</i> – inclusive design	WCAG 2.1; ISO 9241-210
6.4.4 Consent Management	Can citizens easily give, view, and revoke consent?	<i>Data and Process</i> – audit trails of consent	GDPR Art. 7; ISO 27701-8.2
6.4.5 Data Accuracy and Integrity	Are data validation, correction, and version-control mechanisms in place?	<i>Tools & Technology and Process</i> – data quality management	ISO 8000; 3000 Paragraph 48
6.4.6 Privacy and Security Protection	Are privacy impact assessments conducted and security controls audited?	<i>Process and Tools & Technology</i> – PIA & ISMS	ISO 27001/ 27701; ISSAI 4000
6.4.7 Citizen Rights Across Lifecycle	Are citizen data rights (access, correction, portability, retention, and deletion) supported by effective technical and procedural controls across the full data lifecycle?	Data Governance and Process – enforcement of rights, lifecycle controls, and accountability mechanisms	GDPR Arts. 15–20; ISO 15489; ISO 27701; National data protection and records management laws

Data Lifecycle Emphasis: Citizen data rights at each phase i.e. creation, access, correction, retention, and deletion, covering the *Deployment and Operations* stages and extending to decommissioning.

Collectively, these objectives provide an integrated basis for audit design and execution by linking institutional, operational, technical, and data governance considerations to measurable public value, inclusion, and accountability outcomes.

6.5 Summary of Key points

- The audit framework groups objectives into three core domains: **Governance of DPI** (institutional structure, strategy, oversight), **Stakeholder Engagement** (collaboration, transparency, market participation) and **Inclusion, Access & Privacy for Citizens** (equitable access and protection of rights).
- **Audit focus should be adapted to the maturity of the DPI ecosystem**, prioritising foundational governance and accountability mechanisms in early-stage systems.
- The objectives connect directly to **data lifecycle stages (creation → use → sharing → retention → deletion)** to ensure continuous accountability and responsible data stewardship.

An abstract graphic of a network or mesh structure, composed of numerous small blue dots connected by thin, light blue lines. The structure is more dense and complex on the left side, tapering off towards the right. It appears to be a stylized representation of a digital or organizational network.

CHAPTER-7

AUDIT DESIGN MATRIX (ADM)

CHAPTER-7

AUDIT DESIGN MATRIX (ADM)

7.1 Purpose and Structure

The **Audit Design Matrix (ADM)** is a structured tool that translates broad audit objectives (from **Chapter 6**) into *specific, testable questions* linked to standards, evidence, and risk. It helps auditors ensure completeness, logical flow, and traceability of findings embodying ISSAI 3000 Paragraphs 38–49 on criteria, evidence, and documentation.

7.2 Sample ADM Entries

Audit Objective	Audit Question	Criteria/ Standard	Evidence Required	Risk if Absent	PPT Dimension	Data Phase
Governance of DPI	Are technology choices guided by open standards and interoperability principles?	ISO 27001, W3C API Guidelines	Technical architecture, RFP docs	Vendor lock-in, incompatibility	Tools & Technology	Development & Use
Governance of DPI	Are technology choices guided by open standards and interoperability principles?	ISO 27001, W3C API Guidelines	Technical architecture, RFP docs	Vendor lock-in, incompatibility	Tools & Technology	Development & Use
Market Fairness & Competition	Are procurement and platform rules designed to avoid monopolies and promote open participation by vendors and innovators?	GUID 5280; OEC Competition Principles, UN Safeguard – Structural Integrity	Procurement policy, RFP evaluation criteria	Vendor lock-in, stifled innovation	Process	Development
Sustainability & Capacity	Are long-term financial, institutional, and human and infrastructural capacity plans in place to sustain DPI operations?	UN DPI Framework; ISSAI 3000 Paragraph 50, UN Safeguard – Structural Integrity	Budget documents, HR plans, training modules, BC/ DR Plans.	Dependency on external entities, service discontinuity	People / Process	Retention & Use
Infrastructure Autonomy & Exit Readiness	Whether a documented cloud exit strategy and data portability plan exists ensuring seamless transition between hosting environments; whether internal teams have sufficient operational capability to sustain DPI independently?	ISO 22301; GUID 5280-7; ISO/ IEC 38500; UN DPI Safeguard – Structural Integrity (Resilience)	cloud hosting contracts, exit clauses, data portability provisions, internal skills assessments, DR test records	Inability to migrate/ recover data on vendor failure; loss of data sovereignty; prolonged service disruption due to internal capability gaps	Process/ Tools Technology	Development & Operations

Audit Objective	Audit Question	Criteria/ Standard	Evidence Required	Risk if Absent	PPT Dimension	Data Phase
Stakeholder Engagement	Do contracts safeguard data ownership and audit rights?	GUID 5280-7; OECD Competition Principles	Contract clauses, procurement records	Data monopoly, transparency loss	Process	Sharing
Stakeholder Engagement	Are grievance mechanisms accessible in multiple languages and formats?	ISO 10002; WCAG 2.1 & accessible users	Grievance portal, user manuals	Exclusion of vulnerable users	People/ Tools & Technology	Use
Inclusion & Privacy	Are accessibility audits conducted periodically?	GDPR Art 5(1)(c); ISO 27701 7.4	Consent forms, system logs	Privacy violation, data over-collection	Data/ Process	Creation
Inclusion & Privacy	Is personal data collected minimally and with informed consent?	WCAG 2.1; ISO 9241-210	Audit reports, test cases	Non-compliance with inclusion mandate	Tools & Technology / People	Use
Trust & Safeguards	Does the DPI ensure mechanisms for transparency, accountability, and citizen trust (e.g., public dashboards, open algorithms)?	UN Safeguard – Safety & Trust; OECD Open Data Charter; ISO 27001 - A.18	Public portals, transparency policies, code publication records	Public mistrust, opacity, reputational loss	Process/ Tools & Technology	Use & Sharing
Rights-Based Design	Are gender equality, accessibility, and data-protection principles integrated into DPI design from inception?	UN Safeguard – Inclusion; GDPR Art 25; WCAG 2.1	Design specifications, test cases, policy drafts	Exclusion, bias, rights violations	People/ Tools & Technology	Creation

7.3 Risk Rating and Severity

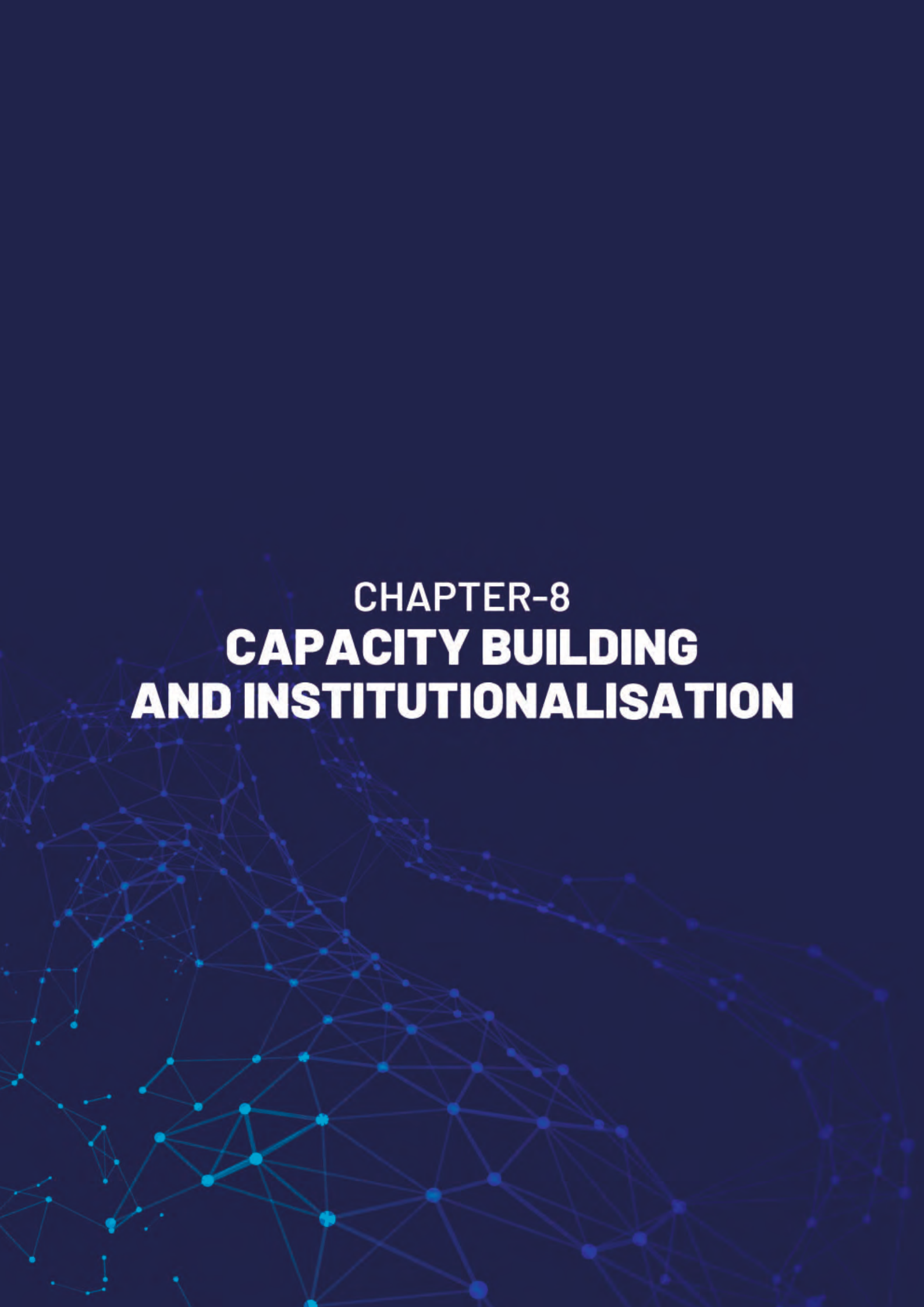
Each ADM row should assign a **risk severity score** based on impact × likelihood:

Rating	Definition	Colour Code	Safeguard Alignment
High	Material effect on citizens' rights or system availability	 Red	<i>UN DPI: Risks to Inclusion / Safety</i>
Medium	Significant but remediable control gap	 Amber	<i>UN DPI: Structural Vulnerabilities (Institutional Weakness, Sustainability)</i>
Low	Minor or process-level weakness	 Green	<i>UN DPI: Lifecycle or Compliance Oversight</i>

Severity classification feeds directly into audit reporting. Auditors should use the severity rating to prioritise findings, structure conclusions, and calibrate the urgency of recommendations. High-severity findings relating to citizens' rights or system availability should be prominently reported with time-bound recommendations; Medium-severity findings should be reported with remediation timelines; Low-severity findings may be consolidated or addressed through management letters. The integrated reporting cycle – covering findings, conclusions, risk-prioritised recommendations, and follow-up tracking – is described in **Chapter 9** (Practical Audit Approach) and illustrated in **Annexure C** (Audit Methodology).

Illustrative sectoral Audit Questions have been provided in **Annexure F** and Audit Questions on Core DPI Components have been provided in **Annexure E**. Auditors should treat **Annexure E** as the component-specific supplement to the ADM as it provides audit questions, PPT&D dimension mapping, evidence types, and reference standards organised by DPI component (Digital Identity Systems, Trust Infrastructure & Authentication, Digital Payments, Data Exchange, and Discovery & Fulfilment).

When populating ADM rows for a specific DPI component-level audit, auditors should draw directly from the relevant **Annexure E** sub-section and adapt those questions to their national context. Typical audit findings will vary by context, DPI maturity, and national legal framework and are therefore left to auditor professional judgement, informed by the risk indicators in **Paragraph 5.4** and the severity classification in **Paragraph 7.3**.

An abstract graphic in the bottom-left corner of the page, consisting of a complex network of interconnected nodes and lines. The nodes are represented by small circles in various shades of blue and teal, while the lines are thin and light blue. The network structure is dense and organic, resembling a molecular or digital web, and it extends diagonally across the lower portion of the cover.

CHAPTER-8

CAPACITY BUILDING AND INSTITUTIONALISATION

CHAPTER-8

CAPACITY BUILDING AND INSTITUTIONALISATION

8.1 Purpose

Digital Public Infrastructure audits require **multi-disciplinary expertise** spanning policy, technology, law, and social inclusion. Without institutional capacity, the standards and methodologies defined earlier cannot be implemented with credibility or consistency. This section provides a roadmap for building enduring capacity in SAIs to conduct DPI audits systematically, in line with the INTOSAI Development Initiative's (IDI) “Whole-of-SAI” capacity-building approach.

8.2 Competency Requirements for DPI Auditors

ISSAI 3000 Paragraph 63 states that “the audit team collectively shall have the necessary professional competence to perform the audit.”

In the context of DPI, this requires both *core audit skills* and *domain-specific expertise*.

Competency Area	Description	Reference Standard/ Framework
Public Sector Auditing	Understanding ISSAI principles, performance and compliance auditing	ISSAI 100, 3000, 4000
Information Systems & Cybersecurity	Evaluating general and application controls, data integrity, and continuity	GUID 5100, ISO 27001, 22301
Data Governance & Privacy	Assessing data lifecycle compliance, privacy-by-design, and consent mechanisms	ISO 27701, GDPR principles
Procurement & Contracting	Reviewing digital procurement, vendor lock-in, and open standards	GUID 5280, Competition Principles
AI and Emerging Technologies	Understanding algorithmic risks, bias, and explainability	OECD AI Principles, ISO/IEC 23894
Inclusion & Accessibility	Applying WCAG and ISO 9241 standards to assess accessibility	WCAG 2.1, ISO 9241-210
Communication & Visualization	Preparing stakeholder-friendly, data-driven audit reports	ISSAI 3000 Paragraph 55–62

A **Competency Matrix** should be maintained by each SAI to identify training needs and ensure balanced team composition (auditor, IT specialist, domain expert, legal adviser, *etc.*).

8.3 Institutionalising Audit-Ready DPI Processes

Institutional readiness ensures that DPI audits are not one-off exercises but **embedded functions** in the SAI's audit plan.

The process involves:

1. **Integrating DPI into the Annual Audit Plan** — Identify high-risk DPI systems (identity, payment, health, education) and schedule rolling audits.
2. **Creating Specialised DPI Audit Cells** — Multidisciplinary teams equipped with IT tools, legal reference databases, and data analysis capacity.
3. **Developing Standard Operating Procedures (SOPs)** — For data collection, privacy handling, and stakeholder communication.
4. **Establishing Knowledge Repositories** — Digital libraries of past audits, ADM templates, and best practices accessible across audit divisions.
5. **Using Secure IT Infrastructure** — For handling sensitive DPI datasets, in line with ISO 27001 and national data-protection laws.
6. **Continuous Quality Assurance** — Periodic internal reviews, peer learning with other SAIs, and alignment with INTOSAI WGITA guidelines.

This aligns with ISSAI 3000 Paragraph 21 on quality control and ISSAI 100's principle of *institutional independence combined with professional responsibility*.

8.4 Tools and Technology Enablement

To support auditors, SAIs should adopt **digital audit platforms** that automate evidence management, risk scoring, and reporting visualisation.

Examples of enabling tools include:

- **Audit Design Matrix (ADM) software** with embedded ISSAI and ISO reference libraries.
- **Data analytics modules** to detect anomalies in DPI transaction logs.
- **Accessibility testing utilities** for website and mobile interface evaluation.
- **Privacy compliance dashboards** integrating automated consent verification and data-retention checks.

SAIs should also be aware of the growing availability of **AI-assisted audit tools** that support DPI-relevant functions, including automated anomaly detection in system logs, network traffic analysis, vulnerability scanning, Security Information and Event Management (SIEM), and Infrastructure-as-Code security assessment. These tools can significantly enhance audit efficiency and coverage, particularly for technically complex DPI systems. SAIs are encouraged to assess and adopt such tools based on their own procurement frameworks, jurisdictional requirements, data sovereignty obligations, and available budget giving preference to tools that support open standards and avoid creating new dependencies or vendor lock-in.

Auditors should receive technical training to use these tools effectively while maintaining ethical safeguards for data confidentiality (ISSAI 130).

8.5 Continuous Professional Development (CPD)

Each SAI should establish a structured CPD program for DPI auditors. Suggested learning streams include:

- **Digital Governance & Ethics** — through IDI or national civil-service academies.
- **Digital Infrastructure, Cybersecurity & Privacy** — *via* ISO-certified training or partnerships with data-protection authorities.
- **Inclusive Design & Accessibility Auditing** — in collaboration with disability commissions or NGOs.
- **AI & Algorithmic Accountability** — in partnership with academic institutions (*e.g.*, IITs, Universities).

CPD credits and certifications help sustain competence and ensure audit credibility in fast-evolving technology environments.

8.6 Collaboration and Knowledge Sharing

INTOSAI promotes *cooperative audits* to share expertise across SAIs. For DPI, the following collaborative avenues are encouraged:

- **WGITA (Working Group on IT Audit)** — to develop DPI-specific methodologies and share ADM templates.
- **IDI (INTOSAI Development Initiative)** — to conduct blended learning programs on digital governance auditing.
- **Regional SAI Groups** (ASOSAI, AFROSAI, EUROSAI, *etc.*) — to share contextual experiences and benchmarks.
- **Academic Partnerships** — with universities and think tanks for AI, privacy, and data lifecycle research.
- **Public Engagement** — inviting civil society and academia for inclusive audit design and post-audit dialogues.

This cooperative model ensures SAIs build *networked capacity*, echoing ISSAI 100's call for “learning from each other to improve global public-sector accountability.”

8.7 Embedding the People–Process–Tools & Technology + Data Lens in Capacity Building

The People, Process, Tools & Technology and Data framework that runs through these Guidelines should also shape capacity development:

Dimension	Capacity Focus	Example Initiatives
People	Skills, ethics, and leadership	Training academies, mentorship, ethical auditing modules
Process	SOPs, workflows, documentation	Standard templates for DPI audits, ADM governance manual
Tools & Technology	Digital enablers and automation	Shared audit software, analytics dashboards, secure cloud
Data Governance	Responsible data handling, privacy safeguards	Data-handling SOPs, anonymisation protocols, PII registers

This ensures that institutional development reinforces audit quality while safeguarding citizen trust.

8.8 Expected Outcomes

Effective capacity building will enable SAIs to:

- Conduct DPI audits consistently using standardised ADM templates;
- Produce globally comparable, evidence-based reports;
- Nurture multidisciplinary audit teams fluent in both policy and technology;
- Collaborate internationally on digital governance assurance; and
- Strengthen citizens' trust in digital transformation through credible oversight.

An abstract graphic in the bottom-left corner of the page, consisting of a complex network of interconnected nodes and lines, resembling a digital or data network. The nodes are small circles, and the lines are thin, creating a web-like structure that extends across the lower portion of the cover.

CHAPTER-9
AUDITING DIGITAL PUBLIC
INFRASTRUCTURE (DPI):
A PRACTICAL AUDIT
APPROACH FOR SAIs

CHAPTER-9

AUDITING DIGITAL PUBLIC INFRASTRUCTURE (DPI): A PRACTICAL AUDIT APPROACH FOR SAIs

9.1 Purpose and Audience

This chapter provides a practical audit guide for Supreme Audit Institutions (SAIs) undertaking audits of Digital Public Infrastructure (DPI), particularly in environments where:

- IT audit capability varies widely,
- DPI systems are evolving or unevenly implemented, and
- Audit teams include many non-technical auditors.

DPI audits cannot be effectively conducted using a single audit lens. Unlike conventional IT systems, DPI cuts across governance, performance, compliance, and information systems, and therefore requires an integrated audit approach, rather than separate or siloed audits. This chapter aims to:

1. Establish a shared and operational understanding of DPI for audit teams.
2. Provide clear guidance for identifying auditable DPI systems within government.
3. Support risk-based audit planning that is feasible, proportionate, and aligned with SAI mandates.

The chapter does not assume advanced IT audit skills. Instead, it focuses on audit judgement, governance understanding, and risk awareness, supported by basic systems knowledge.

9.2 What is DPI for Audit Purposes?

For audit purposes, Digital Public Infrastructure refers to foundational digital systems that:

- operate at population or ecosystem scale,
- enable multiple public and private actors to deliver services, and
- are governed through common standards, rules, and safeguards.

DPI is not defined by technology alone. Its defining characteristics are reusability, interoperability, and public-interest governance. From an information-systems perspective, DPI typically performs one or more of the following core functions:

- identity, authentication, or trust services;
- financial or non-financial transaction enablement;
- data exchange or interoperability across institutions; or
- platform-level enablement for service delivery across sectors.

Importantly, not all large IT systems qualify as DPI. A system used internally by a single organisation, even if technologically advanced, does not constitute DPI unless it enables cross-organisational use, shared standards, and ecosystem participation. This distinction is critical to prevent DPI audits from being diluted into general IT or ERP reviews.

9.3 Audit Orientation: An Integrated Approach

Auditing DPI requires a hybrid audit configuration, combining:

- strengths in governance, performance, and public-value assessment; and
- expertise in systems, controls, cybersecurity, and data integrity.

A DPI audit should be planned and executed as one integrated engagement, not as parallel audits. Audit objectives, scope, evidence standards, and reliance strategies should be jointly agreed by the audit team at the planning stage.

This integrated orientation is especially important where DPI systems are:

- evolving or fragmented,
- partially outsourced, or
- implemented unevenly across sectors or regions.

9.4 Initial Scoping and Risk Assessment

Before finalising audit objectives or the Audit Design Matrix (ADM), audit teams should undertake a structured scoping exercise.

Identifying Material Risks

Once a system qualifies as Digital Public Infrastructure, auditors should identify material risk areas aligned with the DPI risk assessment framework. These typically include:

- **inclusion risks**, relating to unequal access, exclusion, or disempowerment of individuals or groups;
- **design risks**, including algorithmic bias, opaque decision-making, and exclusionary system or interface design;
- **data governance risks**, covering privacy protection, consent management, data minimisation, and secure, purpose-bound data use;
- **operational risks**, including vendor dependency, sustainability, cybersecurity, and system resilience; and
- **accountability risks**, including clarity of ownership, oversight, and redress across public and private actors.

The objective of this identification is risk prioritisation, not exhaustive technical enumeration.

9.5 Risk-Based Audit Planning

After scoping, the audit focus should shift from classification to **risk-based planning**. Because DPI operates at ecosystem or population scale, weaknesses are rarely confined to a single organisation. Audit teams should therefore focus on risks that threaten public value, accountability, or trust, rather than attempting comprehensive system testing.

Based on risk assessment, the audit team should deliberately choose the audit orientation:

- governance-led,
- performance-led, or

- hybrid.

9.6 Jurisdiction, Accountability, and Public–Private Interfaces

DPI systems rarely fall under the control of a single organisation. Auditors should therefore **map accountability across the DPI ecosystem**, distinguishing:

- system designers,
- operators,
- regulators or overseers, and
- service-delivery users.

Where parts of the ecosystem fall outside audit jurisdiction, auditors should not attempt to audit those entities directly. Instead, the audit should assess whether auditable public entities have:

- defined clear governance and oversight arrangements;
- established accountability and reporting mechanisms; and
- put in place controls to manage third-party or cross-jurisdictional risks.

Private participation does not dilute public responsibility. Weaknesses at public–private interfaces should be reported as governance and risk-management issues, not merely contractual or technical failures.

9.7 Executing DPI Audits: Evidence and Methods

In cases where the DPI audits are evidence-driven but not technology-intensive, auditors should plan to triangulate evidence from:

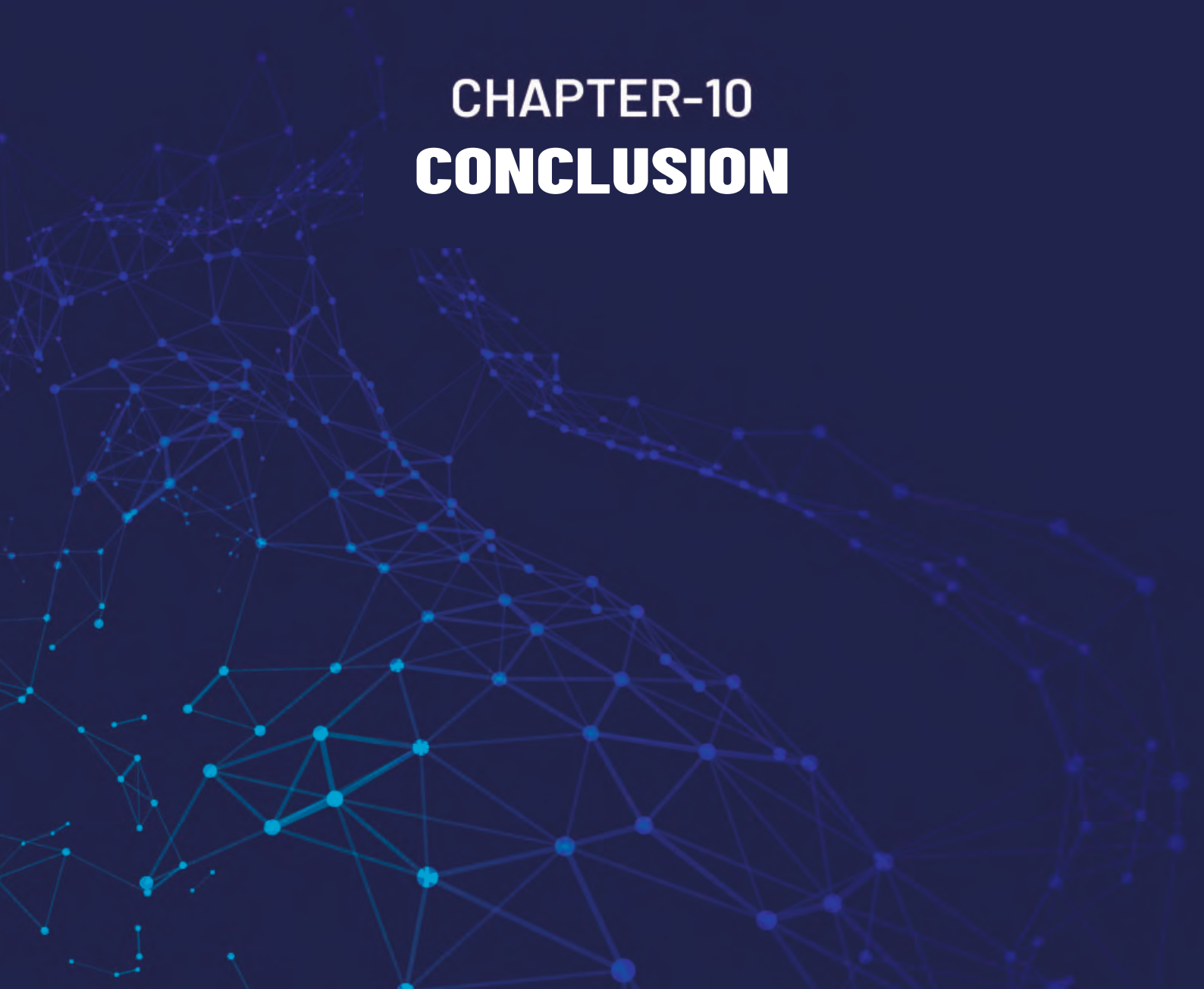
- policies, legal frameworks, and governance records;
- system documentation, contracts, and service-level agreements;
- performance and usage data; and
- grievance redressal and incident-management records.

Where system access is available, auditors may review selected logs or reports, but such testing should be risk-focused and proportionate. Constraints in access or technical capability should be documented transparently and reflected in the audit design, rather than treated as barriers to undertaking the audit.

Audit findings should clearly distinguish between:

- design weaknesses (*e.g.*, unclear accountability or safeguards); and
- implementation weaknesses (*e.g.*, poor enforcement or monitoring).

Recommendations should be realistic and phased, particularly in low-maturity DPI environments.

An abstract graphic of a network or mesh structure, composed of numerous small blue dots connected by thin, light blue lines. The structure is more dense and complex on the left side, tapering off towards the right. It appears to be a stylized representation of a molecular structure or a data network.

CHAPTER-10

CONCLUSION

CHAPTER-10

CONCLUSION

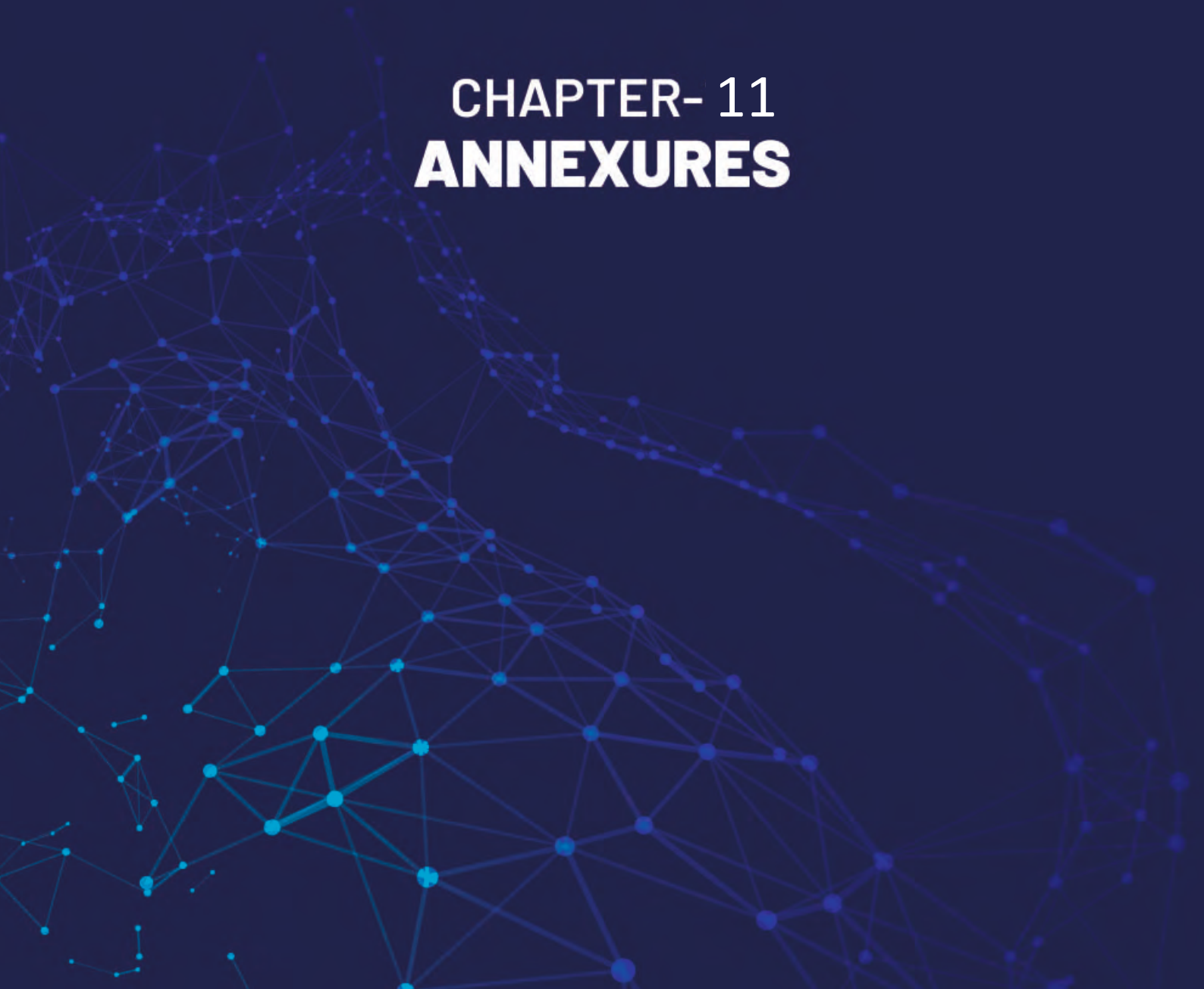
Digital Public Infrastructure (DPI) represents both a technological milestone and a governance challenge. It has the power to redefine how citizens interact with the state enabling inclusion, transparency, and innovation at an unprecedented scale. Yet, without clear accountability and ethical safeguards, it also risks deepening inequalities and compromising trust in public institutions.

This **Audit Guideline for Digital Public Infrastructure** provides a comprehensive framework for SAIs to examine DPI ecosystems through the combined lenses of **People, Process, Tools & Technology, and Data Governance**. Built upon the foundations of ISSAI 100, 130, 3000, and 4000, and supported by GUID 5100 (Information Systems Audit) and GUID 5280 (Public Procurement Audit), it integrates international best practices from ISO, OECD, ITU, W3C, and GDPR-aligned data frameworks.

Aligned with the **UN Universal DPI Safeguards Framework (2024)**, these Guidelines emphasise that auditing DPI is not merely an exercise in detecting non-compliance, but an assurance mechanism for public value, ensuring that digital transformation remains human-centred, rights-respecting, inclusive, and sustainable. By embedding audit objectives into a structured **Audit Design Matrix (ADM)** linked to DPI lifecycle stages, SAIs can produce evidence-based insights that strengthen governance and empower citizens.

As digital systems evolve, so too must the audit profession. Continuous learning, collaboration among SAIs, and the responsible use of emerging technologies such as AI- assisted auditing will be essential to maintain relevance and authority. In doing so, SAIs affirm their enduring constitutional mandate: to protect public trust, ensure accountable governance, and uphold the principles of **economy, efficiency, effectiveness, equity and ethical integrity** in the digital age.

Ultimately, these Guidelines reaffirm that inclusion and accessibility are not peripheral to public audit they are the measure of its success.

An abstract graphic in the bottom-left corner of the page. It consists of a complex network of small, light-blue dots connected by thin, light-blue lines. The network forms a dense, irregular shape that tapers off towards the right, resembling a stylized map or a data visualization of a network.

CHAPTER- 11

ANNEXURES

CHAPTER-11

ANNEXURES

11.1 Purpose of Annexures

These annexures provide *ready-to-use artefacts* for auditors and training institutions. They serve three main functions:

1. **Operationalisation** – convert principles into day-to-day tools;
2. **Standardisation** – enable comparability across SAIs and jurisdictions; and
3. **Capacity Building** – serve as practical learning resources within IDI and WGITA programs.

11.2 Updating and Maintenance

Given rapid evolution in technology and governance, SAIs should treat these annexures as **living instruments**.

They should be reviewed periodically to incorporate:

- 1 New standards (*e.g.*, AI governance, quantum security),
- 1 Emerging DPI use cases (health, education, climate data), and
- 1 Lessons from global cooperative audits.

Annexure A – Glossary of Key Terms

Term	Definition (for Audit Purposes)	Primary Source
Accessibility	The degree to which digital systems can be used by persons with diverse abilities, languages, literacy levels, devices, and connectivity conditions.	WCAG 2.1; ISO 9241
Accountability Risk	The risk arising from weak oversight, unclear ownership, ineffective redressal mechanisms, or fragmented governance structures across public–private DPI actors, including monopoly control over critical DPI components and uncoordinated digital initiatives.	ISSAI 100; ISSAI 130; UN DPI Safeguards Framework
AI-Assisted Audit Tools	Software tools that apply artificial intelligence to support audit functions, including automated anomaly detection in system logs, network traffic analysis, vulnerability scanning, Security Information and Event Management (SIEM), and Infrastructure-as-Code security assessment, used within DPI audit engagements.	GUID 5100; OECD AI Principles; ISO/ IEC 23894
Algorithmic Governance	The set of policies, standards, and oversight mechanisms that govern the design, deployment, monitoring, and accountability of automated decision-making and AI-driven processes within DPI systems, including requirements for Transparency, Explainability, Bias testing, and Human-in-the-loop controls.	OECD AI Principles (2019, updated 2024); ISO/ IEC 23894:2023
Audit Design Matrix (ADM)	A structured audit planning and execution tool that links audit objectives, audit questions, criteria, risks, evidence, and methodology, ensuring traceability and compliance with ISSAI requirements.	ISSAI 3000 Paragraphs 35–49
Auditability	The extent to which DPI systems generate traceable, reliable, and verifiable records such as logs and audit trails that are suitable for independent audit examination.	ISSAI 3000
Building Blocks	Modular, reusable, and interoperable digital components that provide core functionalities (such as identity, authentication, payments, or data exchange) and can be combined to form scalable DPI systems.	GovStack Framework; World Bank
Business Continuity Planning (BCP)	Planning and controls to ensure that DPI services can continue or be rapidly restored following disruptions.	ISO 22301
Citizen Registry	A foundational DPI component in which each individual is uniquely identifiable through a trusted digital identity, enabling secure access to services across multiple platforms using biometric, demographic, or federated identity systems.	DPI Audit Guidelines Paragraph 2.3

Term	Definition (for Audit Purposes)	Primary Source
Citizen-Centric Design	A design approach that prioritises citizens' needs, rights, accessibility, inclusion, and ease of use over organisational or technological convenience.	OECD Digital Government Principles
Cloud Exit Strategy	A documented plan that ensures a DPI system can be migrated between hosting environments or cloud providers without loss of data sovereignty, service continuity, or operational capability, including data portability provisions and internal team readiness assessments.	ISO 22301; GUID 5280-7; ISO/ IEC 38500; UN DPI Safeguards – Structural Integrity
COBIT 2019	An IT governance, management, and assurance framework maintained by ISACA that provides control objectives for IT governance, risk management, and service delivery. It may serve as a complementary reference criterion alongside GUID 5100 and relevant ISO standards in DPI audits.	ISACA
Competency Matrix	A structured tool maintained by each SAI to map the multi-disciplinary skills required for DPI auditing — including public sector auditing, information systems, cybersecurity, data governance, procurement, AI, and inclusion — against team members, identifying training gaps and enabling balanced team composition.	ISSAI 3000 Paragraph 63; DPI Audit Guidelines Paragraph 8.2
Compliance Audit	An audit type defined under ISSAI 4000 that verifies conformity with applicable laws, data-protection regulations, procurement rules, accessibility standards, and other legal or regulatory obligations relevant to DPI systems.	ISSAI 4000
Consent Management	Technical and procedural mechanisms that allow citizens to give, view, modify, and revoke their consent for collection and use of personal data within DPI systems, with audit trails maintained for each consent action.	GDPR Art. 7; ISO/ IEC 27701-8.2; UN DPI Safeguards Framework
Consent-Based Data Sharing	A data-sharing model in which individuals explicitly authorise how their personal data is accessed, used, and shared across DPI systems.	OECD; UN DPI Safeguards Framework
Continuous Professional Development (CPD)	A structured program of ongoing learning for DPI auditors covering digital governance and ethics, cybersecurity and privacy, inclusive design, AI accountability, and emerging technology, enabling sustained competence in a fast-evolving DPI environment.	ISSAI 3000 Paragraph 63; DPI Audit Guidelines Paragraph 8.5

Term	Definition (for Audit Purposes)	Primary Source
Cooperative Audit	A coordinated audit exercise conducted jointly or in parallel by two or more Supreme Audit Institutions on the same or closely related DPI system, cross-border digital initiative, or shared programme, using common frameworks, criteria, and timelines, while each SAI retains authority over its own findings and report.	INTOSAI; ISSAI 100; DPI Audit Guidelines Paragraph 8.6
Data Accuracy	The degree to which data within DPI systems correctly represents real-world entities or events and is maintained through validation and correction mechanisms.	ISO 8000
Data Exchange	One of the five core DPI building blocks, enabling consent-based, interoperable transfer of data between government agencies, private entities, and citizens through standardised APIs and data-sharing protocols.	DPI Audit Guidelines Paragraph 2.1; GovStack Framework
Data Governance	The framework of policies, roles, standards, and controls governing how data is created, used, shared, retained, archived, and disposed of within DPI systems.	OECD Data Governance Framework; UN DPI Safeguards Framework
Data Governance Lifecycle	A lifecycle-based view of data management covering creation, use, sharing, retention, archival, and disposal, adopted in these Guidelines for audit planning and evidence mapping.	ISO 15489; OECD
Data Governance Risk	The risk arising from weaknesses in the management of the data lifecycle, leading to privacy violations, surveillance, or loss of user agency, including inadequate consent mechanisms, excessive data retention, and insecure or non-purpose-bound data sharing.	ISO/ IEC 27701; ISO 15489; UN DPI Safeguards Framework
Data Minimisation	The principle that DPI systems should collect and process only the data that is strictly necessary for a defined and lawful purpose.	GDPR Art. 5
Data Portability	The ability of users or public entities to transfer, export, or migrate data from one DPI system or hosting environment to another without loss of integrity, enabling data sovereignty, competition, and continuity in the event of vendor failure or system transition.	GDPR Arts. 15–20; ISO/ IEC 38500; GUID 5280-7
Data Protection Authority (DPA)	An independent public body responsible for overseeing compliance with data protection laws, enforcing rights of data subjects, and providing guidance on lawful data processing within DPI ecosystems.	GDPR; National data protection laws

Term	Definition (for Audit Purposes)	Primary Source
Decommissioning and Archival	The final phase of the DPI lifecycle covering the secure closure of a system, including data retention per applicable schedules, irreversible deletion of data that has reached end-of-life, and long-term preservation of records required for accountability, in accordance with ISO 15489 and ISO 27040.	ISO 15489; ISO 27040; DPI Audit Guidelines Paragraph 6.1
Design Risk	The risk arising from system or algorithmic design choices — including bias, opacity, or exclusionary interfaces — that cause harm to users, including automated decisions without explainability, inaccessible user interfaces, and absence of human-in-the-loop controls.	OECD AI Principles; ISO/ IEC 23894; UN DPI Safeguards Framework
DFOG (Duplication, Fragmentation, Overlap, and Gaps)	A diagnostic lens used in DPI audits to identify systemic governance weaknesses across institutional mandates and data flows, where responsibilities are duplicated, services are fragmented, oversight overlaps without coordination, or accountability gaps exist across agencies.	DPI Audit Guidelines Paragraph 1.5; OECD Whole-of-Government Framework
Digital Ecosystem	A network of public, private, and civil-society actors interacting through shared digital infrastructure, standards, and governance arrangements enabled by DPI.	OECD; UN DPI Safeguards Framework
Digital Identity	One of the five core DPI building blocks providing a unique, verifiable digital credential for individuals and entities — including biometric or demographic-based eID and authentication services — enabling secure, population-scale access to public and private services.	DPI Audit Guidelines Paragraph 2.1; ISO 29115
Digital Literacy	The capacity of citizens and public servants to access, understand, evaluate, and use digital services effectively, including DPI platforms. Low digital literacy is a recognised inclusion risk that can exclude vulnerable populations from DPI-enabled services.	UN DPI Safeguards Framework; OECD
Digital Payments	One of the five core DPI building blocks comprising interoperable payment rails and platforms that enable real-time, account-to-account transactions at population scale (e.g., UPI, Pix), supporting financial inclusion and welfare delivery.	DPI Audit Guidelines Paragraph 2.1; G20 DPI Consensus
Digital Public Goods (DPGs)	Open-source software, open standards, open data, and open digital components that adhere to privacy, security, and 'do no harm' principles and support public value and sustainable development objectives when deployed within DPI ecosystems.	Digital Public Goods Alliance (DPGA)

Term	Definition (for Audit Purposes)	Primary Source
Digital Public Infrastructure (DPI)	Foundational, interoperable digital systems and shared platforms (such as digital identity, payments, data exchange, trust and discovery mechanisms) that operate at population or ecosystem scale to enable inclusive, secure, and efficient delivery of public and private services.	G20 DPI Consensus (2023); OECD; UN DPI Safeguards Framework
Digital Sovereignty	The capacity of a government or institution to maintain independent control over its digital infrastructure, data, and standards — including the ability to operate DPI systems without undue dependence on foreign vendors, proprietary platforms, or external technology ecosystems.	UN DPI Safeguards Framework; OECD
Digital Stack	A layered arrangement of interoperable digital systems — such as identity, payments, data exchange, and trust infrastructure — designed to function together as shared public infrastructure.	World Bank Digital Stack Framework
Discovery and Fulfilment	One of the five core DPI building blocks comprising registries, directories, and cataloguing systems (such as ONDC-like components) that enable citizens and institutions to discover available services and complete end-to-end service transactions.	DPI Audit Guidelines Paragraph 2.1; CDPI DPI Wiki
e-Government	An early stage of digital public administration, focused on digitising departmental services within individual agencies, prior to the development of shared DPI platforms enabling cross-sectoral interoperability.	OECD Digital Government Framework; DPI Audit Guidelines Paragraph 2.2
Economy, Efficiency, Effectiveness, Equity, and Ethical Integrity (SEEs)	The five public value dimensions used in these Guidelines to evaluate DPI outcomes: Economy (efficient use of shared resources), Efficiency (automated, standards-driven processes), Effectiveness (achievement of policy outcomes), Equity (equitable access for all groups), and Ethical Integrity (upholding privacy, fairness, and transparency in data use and algorithmic design).	ISSAI 3000; ISSAI 100; DPI Audit Guidelines Paragraph 2.7
Exclusion Risk	The risk that certain individuals or population groups are systematically denied access to, or benefit from, DPI-enabled services due to design choices, technical barriers, affordability constraints, or structural digital divides, thereby undermining the inclusivity objectives of DPI.	UN DPI Safeguards Framework; OECD
Federated Architecture	An architectural model in which multiple autonomous systems interoperate through common standards while retaining independent governance, ownership, and operational control.	UN DPI Safeguards Framework; World Bank

Term	Definition (for Audit Purposes)	Primary Source
Government as a Platform (GaaP)	A governance model in which government provides shared digital infrastructure, rules, and standards that enable multiple actors to innovate and deliver services.	OECD
Grievance Redressal Mechanism (GRM)	Formal institutional and technical processes that allow users to report issues, seek correction, and obtain remedies related to DPI services, access, or data use.	UN DPI Safeguards Framework
Hybrid Methodology	An audit approach that combines elements of two or more standard audit types — performance, compliance, and information systems audit — applied concurrently or sequentially within a single DPI audit engagement to evaluate systems in their full institutional and technical context.	ISSAI 100; ISSAI 3000; GUID 5100; DPI Audit Guidelines Paragraph 5.1
Inclusion	The extent to which DPI systems ensure equitable access and participation for all individuals, particularly marginalised or vulnerable groups.	UN DPI Safeguards Framework
Inclusion Risk	The risk that certain population groups are excluded from DPI-enabled services due to design choices, access barriers, affordability, or digital divides.	UN DPI Safeguards Framework
Information Systems Audit	An audit type defined under GUID 5100 that examines IT controls, data reliability, system integrity, cybersecurity, and continuity mechanisms underpinning DPI platforms, including general controls (governance, security, continuity) and application controls (input, processing, output).	GUID 5100; GUID 5101
Integrated Approach	An audit strategy that simultaneously examines the People, Process, Tools & Technology, and Data Governance dimensions of DPI systems within a single coordinated audit engagement, ensuring that findings across all dimensions are coherent, cross-referenced, and capable of informing governance improvements.	DPI Audit Guidelines (PPT&D Framework); ISSAI 3000; GUID 5100
Interoperability	The ability of different systems, organisations, and applications to exchange, interpret, and reuse data through agreed standards, protocols, and interfaces.	ITU; W3C
ITIL 4	A widely adopted best-practice framework for IT service management covering service design, transition, operations, and continual improvement. It provides a useful reference lens for assessing structured practices such as service continuity, incident management, change control, and service-level monitoring in DPI contexts, complementary to GUID 5100 and ISO standards.	AXELOS; DPI Audit Guidelines Paragraph 4.9

Term	Definition (for Audit Purposes)	Primary Source
Legacy System Integration	The process of connecting existing or monolithic systems with modern, interoperable DPI components while preserving data integrity and service continuity.	World Bank
Legal Risk	A cross-cutting DPI risk category referring to the potential for legal disputes, regulatory non-compliance, or unenforceable accountability arising from gaps in enabling legislation, ambiguity in liability between public and private DPI actors, jurisdictional uncertainties in cross-border data flows, and absence of legally enforceable citizen rights regarding automated decisions.	ISSAI 4000; GDPR; DPI Audit Guidelines Paragraph 5.4
Maturity-Based Adaptation	The calibration of audit objectives, criteria, and procedures to the maturity of the DPI environment under review — including pilot or early-implementation DPI, nascent regulatory institutions, private-sector-dominated delivery models, and ecosystem interdependency contexts — ensuring that audit findings remain proportionate, risk-responsive, and actionable.	ISSAI 3000 Paragraph 35; DPI Audit Guidelines Paragraph 6.1
Open API	A publicly documented application programming interface that allows standardised and reusable interaction between DPI platforms and external systems.	GovStack Framework
Open Standards	Publicly available technical specifications developed through transparent and consensus-based processes and free from proprietary restrictions, enabling vendor neutrality and interoperability.	ITU; W3C
Operational Resilience	The ability of DPI systems to withstand, adapt to, and recover from disruptions while continuing to deliver essential services.	OECD; ISO 22301
Operational Risk	Risks arising from system operation and ecosystem dependencies, including vendor lock-in, absence of continuity and disaster recovery planning, cybersecurity incidents, single points of failure, absence of a documented cloud exit strategy, and insufficient internal operational capability to sustain DPI infrastructure independently of vendors.	ISO/ IEC 27001; ISO 22301; GUID 5280; UN DPI Safeguards Framework
Parallel Audit	A coordinated audit exercise in which two or more Supreme Audit Institutions independently audit the same or closely related DPI system, programme, or cross-border digital initiative, using a shared audit framework, common criteria, and synchronised timelines, while each SAI retains full sovereignty over its own findings and report.	INTOSAI; ISSAI 100

Term	Definition (for Audit Purposes)	Primary Source
People–Process–Tools & Technology (PPT)	An analytical framework used in these Guidelines to assess institutional capacity (People), governance and operational workflows (Process), and enabling digital systems (Tools & Technology) within DPI audits.	DPI Audit Guidelines (Guiding Philosophy); ISSAI 3000
People–Process–Tools & Technology and Data Governance (PPT&D) Framework	The primary analytical framework of these Guidelines used to assess institutional capacity (People), governance and operational workflows (Process), enabling digital systems (Tools & Technology), and the complete data lifecycle (Data Governance) within DPI audits. Data Governance is the fourth equal pillar, introducing a time dimension to audit analysis.	DPI Audit Guidelines Paragraph 1.5; ISSAI 3000
Performance Audit	An audit type defined under ISSAI 3000 that evaluates the economy, efficiency, and effectiveness of DPI systems in achieving inclusion, accessibility, and intended service outcomes.	ISSAI 3000
Physical Infrastructure Layer	The foundational technical layer of DPI architecture comprising telecommunications networks, data centres, cloud infrastructure, end-user devices, and basic cybersecurity controls that provide the substrate required for all higher-level DPI components to function.	DPI Audit Guidelines Paragraph 2.3
Planning Memorandum	A formal audit planning document that records audit objectives and sub-objectives, expected outcomes, resource plan and skill mix, applicable standards and criteria, and the stakeholder map of responsible entities and intended users, prepared at the outset of each DPI audit engagement.	ISSAI 3000 Paragraphs 23–24; DPI Audit Guidelines Paragraph 5.2
Platform Government	A stage of digital governance in which public services are delivered through shared platforms and registries across agencies.	OECD Digital Government Framework
Platform vs Protocol	A design distinction where platforms centralise control and participation, whereas protocols define open rules enabling decentralised ecosystem participation, relevant for assessing openness and competition in DPI.	World Bank; UN DPI Safeguards Framework
Privacy Impact Assessment (PIA)	A structured process for identifying, assessing, and mitigating privacy risks associated with DPI system design, data flows, and processing activities, conducted prior to system launch and at significant changes, consistent with GDPR Article 35 and ISO/ IEC 27701.	GDPR Art. 35; ISO/ IEC 27701; DPI Audit Guidelines Paragraph 6.4.6

Term	Definition (for Audit Purposes)	Primary Source
Privacy-by-Design	The integration of privacy and data-protection safeguards into the design and operation of DPI systems from inception, rather than as an afterthought.	GDPR Art. 25; ISO/ IEC 27701
Public Value Assurance	A function of DPI auditing that tests whether digital transformation truly advances economy, efficiency, effectiveness, equity, and ethical integrity — verifying that digital systems deliver measurable benefit to citizens and society, not merely technical compliance.	ISSAI 100; ISSAI 3000; DPI Audit Guidelines Paragraph 1.2
Public–Private Interface	The governance and operational boundary where government-provided DPI is accessed, used, or extended by private or non-state actors.	OECD
Purpose Limitation	The data protection principle requiring that personal data collected within DPI systems be used only for the specific, explicitly stated purposes for which consent was obtained, and not further processed in ways incompatible with those purposes.	GDPR Art. 5(1)(b); ISO/ IEC 27701; UN DPI Safeguards Framework
Records Management	The systematic control of the creation, maintenance, retention, and disposal of records generated by DPI systems.	ISO 15489
Risk-Based Audit Planning	An audit approach that prioritises audit focus based on the likelihood and impact of risks to audit objectives, rather than exhaustive coverage of all controls.	ISSAI 100; ISSAI 3000
Safeguards Framework	A structured set of principles, processes, and practices designed to mitigate risks to safety, rights, inclusion, and sustainability in DPI systems.	UN Universal DPI Safeguards Framework
Security-by-Design	The practice of embedding security controls and threat-mitigation measures into system architecture and development processes from the outset.	ISO/ IEC 27001
Service Continuity	The sustained availability and reliability of DPI-enabled services over time, including during emergencies or system failures.	ISO 22301
Service Provider Registry	A foundational DPI component in which public and private entities seeking to deliver services on the DPI are registered, authenticated, and verified against statutory credentials and eligibility criteria established by the DPI's governing authority.	DPI Audit Guidelines Paragraph 2.3
Supreme Audit Institution (SAI)	An independent public body mandated under national law and ISSAI principles to provide assurance that governments use public resources efficiently, legally, and in the public interest. In the digital era, SAIs extend this mandate to auditing DPI ecosystems for inclusion, accountability, data governance, and public value.	ISSAI 100; INTOSAI

Term	Definition (for Audit Purposes)	Primary Source
System-of-Systems	A collection of independent yet interconnected systems that interact to deliver combined functionality, characteristic of DPI ecosystems.	INCOSE
Transparency	The availability of clear, accessible information on DPI governance, rules, data use, and system performance to stakeholders and citizens.	ISSAI 100; OECD
Trust Infrastructure	One of the five core DPI building blocks comprising technical and governance mechanisms — such as authentication, digital signatures, and public key infrastructure (PKI) — that enable secure and reliable interactions within DPI ecosystems.	World Bank; UN DPI Safeguards Framework; DPI Audit Guidelines Paragraph 2.1
UN Universal DPI Safeguards Framework (2024)	A normative global reference developed by the United Nations setting out 18 foundational and operational principles and 13 interrelated risk categories for the design and governance of DPI systems across three dimensions — inclusion, safety, and structural vulnerabilities — covering the full DPI lifecycle from conception through operations.	United Nations (2024)
Vendor Lock-in	A situation in which dependence on proprietary technologies, platforms, or contracts restricts interoperability, portability, competition, or future system choices.	OECD; World Bank
Whole-of-Government Lens	An audit perspective that examines DPI risks and governance weaknesses across multiple agencies, budget lines, and policy frameworks rather than within any single DPI system, enabling auditors to identify systemic causes of exclusion, fragmentation, or accountability gaps arising from uncoordinated digital initiatives.	OECD Whole-of-Government Framework; ISSAI 3000; DPI Audit Guidelines Paragraph 5.4

Annexure B – Mapping of DPI Processes to Data Lifecycle Phases

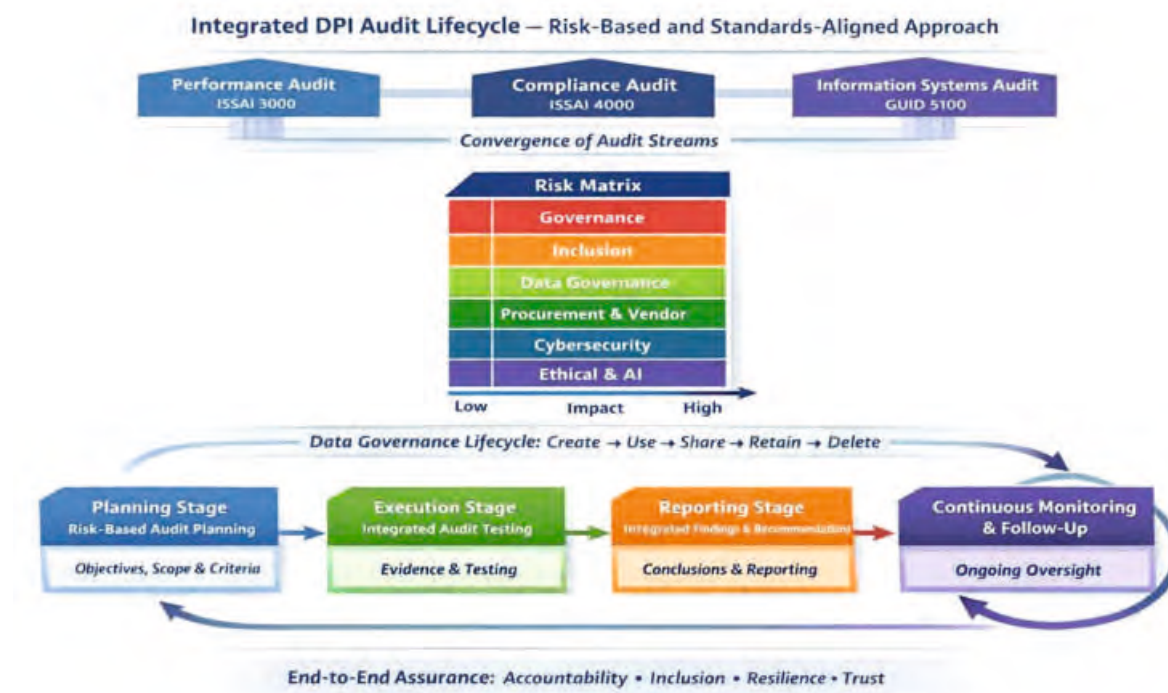
DPI Process	Data Phase	Key Controls/ Audit Focus	Aligned UN DPI Safeguard Dimension
Registration/ Onboarding	Creation and Collection	Consent collection, data minimisation	<i>Safety & Inclusion</i> – informed consent, equitable access
Authentication/ Transactions	Use and Processing	Encryption, access logs, authorisation	<i>Safety</i> – privacy, security, data integrity
Inter-agency Data Exchange	Sharing and Disclosure	API security, data-sharing agreements	<i>Structural Integrity</i> – interoperability, accountability
Storage and Maintenance	Storage and Retention	Backup integrity, retention policy	<i>Structural Integrity</i> – resilience, sustainability
Long-term Records Management	Archival and Preservation	Long-term preservation; Integrity checks; Access controls; Records management	<i>Safety & Accountability</i> — <i>Transparency; Auditability</i>
Decommissioning / End of Life	Deletion and Disposal	Irreversible erasure; Deletion audit trails; Right to erasure; Secure closure; Certificate of destruction	<i>Safety & Accountability</i> — <i>Privacy protection; Lawful disposal</i>

This table anchors the lifecycle dimension across ADM entries and reporting.

ANNEXURE C – AUDIT METHODOLOGY

Figure 9 illustrates the integrated audit approach for the DPI encompassing the planning, execution, reporting and follow up.

Figure 9: Integrated Approach for DPI



This annexure presents a consolidated reference model for auditing Digital Public Infrastructure (DPI) using an integrated, risk-based approach aligned with **ISSAI 3000, ISSAI 4000, and GUID 5100**. Audit focus is determined through a **Risk Matrix** that assesses DPI-specific risks based on impact and likelihood, including governance, inclusion, data governance, procurement and vendor dependencies, cybersecurity, and ethical or AI-related risks. The risk assessment guides the selection and weighing of performance, compliance, and information systems audit lenses and informs the allocation of audit effort across **People, Process, Tools & Technology, and Data Governance**, with due consideration to the data lifecycle from creation to deletion.

Based on this risk-aligned planning, audit execution applies proportionate procedures to assess outcomes and inclusion, legal and regulatory compliance, and the reliability, security, and integrity of DPI systems. Evidence gathered across audit lenses is integrated at the reporting stage to present clear findings, conclusions, and risk-prioritised recommendations, explicitly linked to the underlying risk categories and lifecycle stages. Given the dynamic nature of DPI ecosystems, audit assurance extends beyond reporting through continuous monitoring and follow-up, including tracking implementation of recommendations, updating risk assessments, and feeding lessons learned into future audit planning. This lifecycle model enables SAIs to provide sustained, adaptive assurance over DPI systems without duplicating the conceptual framework set out in the main report.

ANNEXURE D – REFERENCES AND BIBLIOGRAPHY

ISSAI and INTOSAI Pronouncements

- ISSAI 100 – Fundamental Principles of Public-Sector Auditing
- ISSAI 130 – Code of Ethics
- ISSAI 3000 – Performance Audit Standard
- ISSAI 4000 – Compliance Audit Standard
- GUID 5100 – Audit of Information Systems
- GUID 5280 – Audit of Public Procurement

ISO and Other Global Standards

- ISO/ IEC 27001 – Information Security Management
- ISO/ IEC 27701 – Privacy Information Management
- ISO 22301 – Business Continuity
- ISO 8000 – Data Quality
- ISO 9241-210 – Human-Centered Design
- ISO 15489 – Records Management
- ISO 27040 – Storage Security

UN and Multilateral Frameworks

- UN Universal Digital Public Infrastructure (DPI) Safeguards Framework (2024) – *UNDP and Office of the UN Secretary-General's Envoy on Technology*
- *UN – The DPI Approach: A Playbook (2023)*
- *UN – Accelerating the SDGs through Digital Public Infrastructure (2022)*
- *G20 New Delhi Leaders' Declaration (2023)* – Commitment to secure, inclusive, and interoperable DPI
- *World Bank – Digital Public Infrastructure and Development: A WBG Approach (2024)*
- *OECD – Digital Public Infrastructure for an Inclusive Future (2023)*

Policy and Regulatory Frameworks

- General Data Protection Regulation (GDPR)
- OECD Data Governance Policy Framework
- OECD Open Government Data Charter
- UNCITRAL Model Law on Public Procurement
- ITU/ W3C Interoperability Standards
- WCAG 2.1 – Web Content Accessibility Guidelines

Reference Cases and Models

- EU eIDAS Regulation
- Singapore SingPass/ MyInfo
- Estonia X-Road
- MOSIP Open-Source Identity Platform

ANNEXURE E – ILLUSTRATIVE AUDIT QUESTIONS ON CORE DPI COMPONENTS

This annexure provides **illustrative audit questions** for examining the **foundational building blocks of Digital Public Infrastructure (DPI)** namely **Digital Identity, Trust Architecture & Authentication, Digital Payments, Data Exchange, and Discovery & Fulfilment**. These components form the backbone of most DPI ecosystems and are common across multiple sectors such as health, education, welfare, and governance. Their reliability, inclusiveness, and security determines the overall integrity of the digital state.

The questions in this annexure are intended to help auditors assess whether these core systems operate with **economy, efficiency, effectiveness, equity, and ethical integrity**, and whether they uphold the values of **trust, transparency, and accountability**.

Scope and Use

Each subsection corresponds to one DPI component and lists specific audit questions aligned to the **People–Process–Tools & Technology–Data (PPT&D)** framework and to international standards such as **ISSAI 3000, ISSAI 4000, GUID 5100/ 5101, and ISO 27001/ 27701/ 8000**.

Auditors may use these questions to:

- Identify and define **audit objectives and sub-objectives** within the Audit Design Matrix (ADM);
- Determine **evidence requirements** (*e.g.*, system logs, policy documents, API reports, user interviews);
- Benchmark national systems against **global good practices** for digital governance and inclusion; and
- Integrate core-component evaluations into **sectoral audits (Annexure F)**.

These questions are **illustrative and adaptive**, designed to be expanded, merged, or tailored according to national mandates, sectoral maturity, and data availability.

Note: Each criterion is cross-referenced to the corresponding **UNDP DPI Safeguards Principle(s)** to ensure alignment with international human-rights and governance standards.

DIGITAL IDENTITY SYSTEMS

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there enabling legislation or policy clearly defining purpose, scope, and oversight of the digital-ID system?	Process/ People	ISSAI 4000 Paragraphs 16–18; ISO 15489; UN DPI Safeguard – Structural Integrity (Governance & Legitimacy)
2	Are enrolment and de-duplication processes transparent and subject to independent validation?	Process/ Data	GUID 5100-3.2; ISO 8000; UN DPI Safeguard – Safety (Do No Harm by Design)
3	Are biometric and demographic data collected using certified devices and secure protocols?	Tools & Technology/ Data	ISO 19794; ISO 27001 A.9; UN DPI Safeguard – Safety (Security & Reliability)
4	Is informed consent obtained from individuals during enrolment and data update cycles?	People/ Process	GDPR Art. 7; ISO 27701 Annex B; UN DPI Safeguard – Safety (Privacy & Data Protection)
5	Are identity records linked to clear retention and deletion policies with audit logs?	Process/ Data	ISO 15489; ISSAI 3000-49; ISO 27701-7.4; UN DPI Safeguard – Structural Integrity (Data Lifecycle Governance)
6	Are mechanisms in place for citizens to correct or update erroneous data through verified channels?	People/ Process	ISSAI 100 Principle A3; ISO 10002; UN DPI Safeguard – Inclusion (Accountability & Redress)
7	Are API interfaces for ID verification (“Know Your Customer”, service access) auditable and rate-limited?	Tools & Technology / Data	W3C API Guidelines; GUID 5101; UN DPI Safeguard – Structural Integrity (Interoperability & Oversight)
8	Are data minimisation and purpose-limitation principles enforced in ID-based transactions?	Process/ Data	ISO 27701-7.4; GDPR Art. 5; UN DPI Safeguard – Safety (Proportionality & Necessity)
9	Are grievance and redressal mechanisms operational for denial of service or identity misuse?	People/ Process	ISO 10002; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Redress & Accountability)
10	Are biometric failure rates and exclusion statistics monitored and publicly reported?	People/ Data	UN SDG 10; ISSAI 3000-49; UN DPI Safeguard – Inclusion (Equity & Inclusion)
11	Are vendor contracts for biometric devices and software auditable and include data-protection clauses?	Process	GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Procurement & Oversight)
12	Is there an independent oversight body for identity governance and breach investigation?	Process/ People	ISSAI 4000-17; OECD Governance Principles; UN DPI Safeguard – Structural Integrity (Governance & Accountability)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/Data)	Reference/ Criteria
13	Are identity verification services accessible to citizens with limited digital literacy or connectivity?	People/ Tools & Technology	<i>WCAG 2.1; UN CRPD Art. 9; UN DPI Safeguard – Inclusion (Accessibility & Usability)</i>
14	Are cross-border recognition and interoperability mechanisms established (where applicable)?	Process/ Data	<i>eIDAS 2.0; ISO 29115; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)</i>
15	Is there a tested business-continuity and disaster-recovery plan for identity databases and authentication nodes?	Process/ Tools & Technology	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Resilience & Continuity)</i>
16	Whether centralised incident logging, system audit trails, and ticketing mechanisms are in place and whether these logs are reviewed periodically and independently?	Tools/ Process	<i>ISO 27001-A.12.4 (Logging and Monitoring), GUID 5100 (General Controls), GUID 5101 (Information Security Audits), UN DPI Safeguards Framework (Structural Integrity — Resilience and Oversight)</i>

TRUST INFRASTRUCTURE & AUTHENTICATION

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is multi-factor authentication (MFA) mandatory for high-risk Transactions and privileged users?	Tools & Technology/ Process	ISSAI 4000 Paragraphs 16–18; ISO 15489; UN DPI Safeguard – Structural Integrity (Governance & Legitimacy)
2	Are authentication factors (password, OTP, biometric, token) periodically rotated and audited for compromise?	Tools & Technology/ Data	GUID 5100-3.2; ISO 8000; UN DPI Safeguard – Safety (Do No Harm by Design)
3	Are session-management and timeout controls configured per best practice for web and mobile apps?	Tools & Technology/ Process	ISO 19794; ISO 27001 A.9; UN DPI Safeguard – Safety (Security & Reliability)
4	Are authentication APIs protected against brute-force and replay attacks through rate limiting and CAPTCHA?	Tools & Technology/ Data	GDPR Art. 7; ISO 27701 Annex B; UN DPI Safeguard – Safety (Privacy & Data Protection)
5	Are digital signatures and certificates issued through licensed certifying authorities and verified at each transaction?	Process/ Tools & Technology	ISO 15489; ISSAI 3000-49; ISO 27701-7.4; UN DPI Safeguard – Structural Integrity (Data Lifecycle Governance)
6	Are authentication logs time-stamped, tamper-evident, and retained for audit purposes?	Data/ Process	ISSAI 100 Principle A3; ISO 10002; UN DPI Safeguard – Inclusion (Accountability & Redress)
7	Are fallback mechanisms for failed authentication accessible, inclusive, and secure (e.g., OTP, helpdesk)?	People/ Tools & Technology	W3C API Guidelines; GUID 5101; UN DPI Safeguard – Structural Integrity (Interoperability & Oversight)
8	Are federated identity and single-sign-on (SSO) arrangements audited for data-sharing and privacy compliance?	Process/ Data	ISO 27701-7.4; GDPR Art. 5; UN DPI Safeguard – Safety (Proportionality & Necessity)
9	Is there periodic testing of authentication systems against vulnerabilities and phishing attacks?	Tools & Technology/ Process	ISO 10002; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Redress & Accountability)
10	Are access rights and privileges reviewed regularly with segregation of duties enforced?	Process/ People	UN SDG 10; ISSAI 3000-49; UN DPI Safeguard – Inclusion (Equity & Inclusion)
11	Are authentication systems integrated with security-information and event-management (SIEM) tools for real-time monitoring?	Tools & Technology/ Data	GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Procurement & Oversight)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT / Data)	Reference / Criteria
12	Is there an incident-response protocol for identity compromise or credential theft?	Process/ Data	<i>ISSAI 4000- 17; OECD Governance Principles; UN DPI Safeguard – Structural Integrity (Governance & Accountability)</i>
13	Are authentication error logs analysed to identify exclusion patterns or technical bias?	Data/ Process	<i>WCAG 2.1; UN CRPD Art. 9; UN DPI Safeguard – Inclusion (Accessibility & Usability)</i>
14	Are vendor SLAs and certifications for authentication modules periodically reviewed?	Process/ Tools & Technology	<i>eIDAS 2.0; ISO 29115; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)</i>
15	Is authentication architecture stress-tested for scalability and availability under peak loads?	Tools & Technology/ Process	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Resilience & Continuity)</i>

DIGITAL PAYMENTS INFRASTRUCTURE

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a national policy or framework defining ownership, regulation, and oversight of digital payment rails?	Process/ People	ISSAI 4000-16; ISO 22301; UN DPI Safeguard – Structural Integrity (Governance & Trust)
2	Are payment systems integrated with trusted identity and authentication layers to prevent fraud?	Tools & Technology/ Data	GUID 5100-4.3; ISO 27001; UN DPI Safeguard – Safety (Security by Design)
3	Are transaction data encrypted, time-stamped, and stored with appropriate retention controls?	Data/ Process	ISO 27040; ISO 15489; UN DPI Safeguard – Safety (Integrity & Data Protection)
4	Are reconciliation and settlement processes automated with exception-handling logs?	Process/ Data	ISSAI 4000-21; ISO 22301; UN DPI Safeguard – Structural Integrity (Transparency & Accountability)
5	Are merchant-onboarding procedures and KYC checks digitally verifiable and periodically audited?	Process/ People	RBI/ FATF Guidelines; ISSAI 3000-38; UN DPI Safeguard – Structural Integrity (Lawfulness & Oversight)
6	Are transaction limits, charges, and service-fee policies transparent and publicly disclosed?	Process/ People	OECD Competition Principles; ISSAI 100; UN DPI Safeguard – Inclusion (Transparency & Explainability)
7	Is fraud-detection system using AI/ML models tested for accuracy and bias?	Tools & Technology/ Process	OECD AI Principles; ISSAI 130; UN DPI Safeguard – Safety (Ethical AI & Accountability)
8	Are incident-response and dispute-resolution processes for failed transactions well defined and timely?	Process/ People	ISO 10002; ISSAI 3000-52; UN DPI Safeguard – Inclusion (Accountability & Redress)
9	Are digital-payment apps certified for security compliance (PCI-DSS or equivalent)?	Tools & Technology/ Data	PCI-DSS; ISO 27001; UN DPI Safeguard – Safety (Security & Assurance)
10	Is there an audit trail for chargebacks, refunds, and failed transactions?	Data/ Process	ISO 15489; ISSAI 4000-21; UN DPI Safeguard – Structural Integrity (Transparency & Traceability)
11	Are API interfaces with banks and fintech partners secured through tokenisation and mutual authentication?	Tools & Technology/ Data	W3C API Security; ISO 27017; UN DPI Safeguard – Structural Integrity (Interoperability & Security)
12	Are cyber-security drills and penetration DPI tests conducted regularly for payment switches and gateways?	Tools & Technology/ Process	ISO 27035; GUID 5101; UN Safeguard – Safety (Resilience & Security)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
13	Are data residency and cross-border transaction rules complied with for international payments?	Process/ Data	ISO 27701; OECD Cross-Border Data Flow Guidelines; UN DPI Safeguard – Structural Integrity (Proportionality & Compliance)
14	Are system-availability and uptime metrics publicly reported to ensure transparency and trust?	People/ Process	ISSAI 3000-49; UN SDG 16; UN DPI Safeguard – Inclusion (Transparency & Resilience)
15	Is business-continuity plan tested for disaster recovery and switch-over between primary and secondary sites?	Process/ Tools & Technology	ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Continuity & Adaptability)

DATA EXCHANGE AND INTEROPERABILITY PLATFORMS

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a national data-exchange policy governing inter-agency and cross-sector data sharing?	Process/ People	ISSAI 3000-36; ISO 27701; UN DPI Safeguard – Structural Integrity (Governance & Trust)
2	Are data-exchange protocols based on open standards (W3C, ITU, ISO 8000) and documented for interoperability?	Tools & Technology/ Data	ISO 8000; W3C Standards; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)
3	Are metadata registries maintained and linked to version-controlled API catalogues?	Data/ Process	ISO 19115; GUID 5100-4.3; UN DPI Safeguard – Structural Integrity (Resilience & Auditability)
4	Are data-sharing agreements formalised through MoUs or digital contracts with audit-access provisions?	Process/ People	GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Oversight & Accountability)
5	Is data classified by sensitivity (public, restricted, confidential) and handled accordingly?	Process/ Data	ISO 27001 A.9; ISSAI 3000-49; UN DPI Safeguard – Safety (Privacy & Data Protection)
6	Are APIs secured through authentication tokens, encryption, and mutual TLS?	Tools & Technology/ Data	W3C API Security; ISO 27017; UN DPI Safeguard – Safety (Security by Design)
7	Is there a data-exchange audit log recording source, recipient, timestamp, and purpose of transfer?	Data/ Process	ISO 15489; GUID 5101; UN DPI Safeguard – Structural Integrity (Traceability & Accountability)
8	Are data quality metrics (completeness, accuracy, timeliness) monitored and published periodically?	Data / Process	ISO 8000; ISSAI 3000-49; UN DPI Safeguard – Inclusion (Transparency & Explainability)
9	Are consent dashboards or data-trust frameworks available for citizens to view and manage their data sharing?	People/ Process	ISO 27701-7.4; GDPR Art. 15; UN DPI Safeguard – Inclusion (Agency & Consent)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
10	Are data-exchange systems tested for scalability and load balancing under peak conditions?	Tools & Technology Process	<i>ISO 22301; GUID 5100-4.3; Integrity (Resilience & Continuity)</i>
11	Are data transfers subject to encryption and integrity checks to prevent tampering or loss?	Tools & Technology/ Data	<i>ISO 27040; ISSAI 4000-21; UN DPI Safeguard – Safety (Integrity & Security)</i>
12	Are cross-border data flows compliant with applicable laws and international agreements?	Process/ Data	<i>OECD Cross-Border Data Flow Guidelines; ISO 27701; UN DPI Safeguard – Structural Integrity (Proportionality & Compliance)</i>

DISCOVERY & FULFILMENT

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a national or sectoral policy defining governance, scope, and operating models for discovery and fulfilment platforms?	Process/ People	ISSAI 4000-16; OECD Governance Principles; UN DPI Safeguard – Structural Integrity (Governance & Trust)
2	Are open registries or directories (e.g., products, services, benefits, jobs) designed using open standards and interoperable APIs?	Tools & Technology/ Data	W3C Open Data Standards; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)
3	Are discovery algorithms transparent, explainable, and periodically audited for bias or manipulation?	Data/ Process	OECD AI Principles; ISSAI 130; UN DPI Safeguard – Inclusion (Fairness & Ethical AI)
4	Is informed user consent obtained, recorded, and auditable before data sharing with discovery engines or fulfilment providers?	Process/ Data	ISO 27701-7.4; GDPR Art. 7; UN DPI Safeguard – Safety (Privacy & Consent)
5	Are fulfilment workflows (e.g., orders, service delivery, grievance closure) traceable with end-to-end audit trails?	Process/ Data	ISO 15489; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Transparency & Accountability)
6	Are service providers and intermediaries vetted and certified through transparent, non-discriminatory onboarding mechanisms?	People/ Process	OECD Competition Principles; UN SDG 8; UN DPI Safeguard – Inclusion (Equity & Access)
7	Do platforms enforce data minimisation and purpose limitation across discovery, matching, and transaction fulfilment stages?	Process/ Data	ISO 27701-7.4; GDPR Art. 5; UN DPI Safeguard – Safety (Proportionality & Necessity)
8	Are APIs and matching protocols open, version-controlled, and accessible to accredited third-party innovators on fair terms?	Tools & Technology/ Data	W3C API Standards; ISO 20022; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
9	Are integrated grievance and feedback mechanisms available for both consumers and service providers?	People/ Process	ISO 10002; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Accountability & Redress)
10	Is real-time performance monitoring (latency, error rates, uptime) implemented and published through public dashboards?	Tools & Technology/ Process	ISSAI 3000-49; ISO 22301; UN DPI Safeguard – Inclusion (Transparency & Public Accountability)
11	Are discovery and fulfilment services accessible to low-connectivity or low-literacy users through multilingual, assisted, or offline modes?	People/ Tools & Technology	WCAG 2.1; UN CRPD Art. 9; UN DP Safeguard – Inclusion (Accessibility & Usability)
12	Are digital agents, chatbots, or automated brokers auditable for fairness, bias, and explainability?	Tools & Technology/ Data	OECD AI Principles; ISSAI 130; UN DPI Safeguard – Safety (Ethical AI & Explainability)
13	Are environmental sustainability parameters (e.g., carbon footprint, energy use) monitored and disclosed for core platform operations?	Process/ Tools & Technology	ISO 14064; UN DPI Safeguard – Structural Integrity (Sustainability & Accountability)
14	Are cross-platform and cross-border fulfilment transactions compliant with competition, consumer, and privacy laws?	Process/ Data	OECD Cross-Border Data Flow Guidelines; ISO 27701; UN DPI Safeguard – Structural Integrity (Proportionality & Compliance)
15	Is there an institutional mechanism coordinating discovery and fulfilment across ministries, regulators, and private networks?	Process / People	ISSAI 4000-17; InDEA 2.0; UN DPI Safeguard – Structural Integrity (Governance & Collaboration)
16	Are inclusion and participation metrics (e.g., women-owned MSMEs onboarded, regional coverage) monitored and publicly reported?	People/ Process	UN SDG 5; UN DP/2024/7-11; UN DPI Safeguard – Inclusion (Equity & Representation)
17	Are fraud detection, dispute resolution, and grievance protocols tested for efficiency, fairness, and accessibility?	Process/ Tools & Technology	ISO 10002; ISO 22301; UN DPI Safeguard – Safety (Security & Resilience)
18	Are API and registry updates subject to independent security testing and formal change-control approval?	Tools & Technology/ Data	ISO 27001; GUID 5100-4.3; UN DPI Safeguard – Safety (Security & Continuity)
19	Is the platform periodically evaluated for socio-economic impact, accessibility, and potential exclusionary effects?	Process/ People	ISSAI 3000-49; UN SDG 10; UN DPI Safeguard – Inclusion (Equity & Impact)
20	Are DPI safeguard principles (privacy-by-design, do-no-harm, inclusion-by-design) embedded in architecture, review, and governance processes?	Process/ Tools & Technology	UN Universal DPI Safeguards Framework (2024); ISSAI 3000-36; UN DPI Safeguard – Safety (Ethical & Rights-Based Design)

The core-component audit questions in this annexure are designed to help Supreme Audit Institutions (SAIs) examine the **digital foundations** that underpin all sectoral applications of Digital Public Infrastructure (DPI). Whether a programme concerns welfare payments, education credentials, or environmental data, the same underlying elements: **identity, trust infrastructure & authentication, payments, data exchange, and discovery & fulfilment** determine its reliability and trustworthiness.

These questions should be viewed as a **toolkit for modular assurance** rather than a fixed checklist. SAIs may apply them:

- **Independently**, to conduct stand-alone audits of individual DPI components such as digital-ID platforms or payment gateways; or
- **Integratively**, by combining them with the sector-specific questions in **Annexure F** to form a complete ecosystem audit that follows data and accountability across boundaries.

When planning such audits, SAIs are encouraged to:

1. Align questions with their **national mandates** and data-access provisions;
2. Use a **risk-based approach**, focusing on components that carry high transaction volume or citizen-impact;
3. Validate findings through **triangulated evidence**; technical logs, policy documents, and stakeholder feedback; and
4. Relate observations back to the five guiding principles of DPI audit: **economy, efficiency, effectiveness, equity, and ethical integrity**.

Together with the following **Annexure F**, this Annexure provides a comprehensive framework for assessing whether the digital foundations of governance truly enhance public value while safeguarding rights, inclusion, and accountability.

ANNEXURE F – ILLUSTRATIVE SECTORAL AUDIT QUESTIONS

This annexure provides **illustrative audit questions** for applying the Digital Public Infrastructure (DPI) Audit Framework to specific service-delivery sectors. It is intended to help Supreme Audit Institutions (SAIs) and auditors contextualise the core principles of economy, efficiency, effectiveness, equity, and ethical integrity within sectoral realities such as health, education, agriculture, and urban governance.

The questions presented here are **not prescriptive**. They serve as reference points that auditors can adapt to their national priorities, mandates, and risk assessments. Each question aligns with the **People–Process–Tools & Technology–Data Governance** dimensions outlined in the main Guidelines and can be linked to relevant audit criteria in the Audit Design Matrix (ADM).

Scope and Use

The domains included reflect areas where DPI is most commonly deployed in public service delivery and where digital systems have a direct bearing on inclusion, accountability, and efficiency.

For each domain, the annexure identifies key DPI elements, typical risks, and example audit questions that can be used during planning or evidence gathering.

Auditors may:

- Select applicable questions during **ADM preparation** in the planning phase;
- Use them to define **evidence requirements** (system logs, contracts, policy documents, interviews); and
- Map them to **standards or criteria** from ISSAI, GUID, or ISO frameworks relevant to that sector.

Each subsequent table summarises sample questions for one sector or domain.

HEALTH

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a legally authorised framework defining ownership, access, and stewardship of digital health data?	Process/ Data	ISSAI 4000 Paragraphs 16–18; ISO 27701-7.4; UN DPI Safeguard – Structural Integrity (Governance)
2	Are patient-consent mechanisms explicit, revocable, and auditable within national privacy law?	People/ Process	GDPR Art. 7; ISO 27701 Annex B; UN DPI Safeguard – Safety (Consent)
3	Are health-record identifiers uniquely linked to national digital identity systems without enabling unauthorised tracking?	Data	ISSAI 3000-38; ISO 29100 Principle 3; UN DPI Safeguard – Safety (Privacy)
4	Do digital-health systems implement role-based access control and log all clinician and administrator activity?	Tools & Technology / Data	ISO 27001 A.9; GUID 5100-4.3; UN DPI Safeguard – Safety (Security & Trust)
5	Are interoperability standards (FHIR, HL7, SNOMED CT) consistently applied across public and private providers?	Process/ Tools & Technology	WHO Digital Health Toolkit; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability)
6	Are API gateways securing data exchange between hospitals, insurers, and labs through authentication tokens and encryption?	Tools & Technology / Data	ISO 27017; W3C API Security Guidelines; UN DPI – Safety (Security & Resilience)
7	Is there a national registry or certification process for tele-medicine and e-pharmacy platforms?	Process	Health IT Regulations; ISSAI 4000-24; UN DPI Safeguard – Structural Integrity (Institutional Oversight)
8	Are data-storage and backup systems located in compliance with data-residency laws and business-continuity norms?	Tools & Technology / Data	ISO 22301; ISO 27040; UN Safeguard – Structural Integrity (Sustainability)
9	Are accessibility and language features (WCAG 2.1, local-language UI, assistive-tech support) integrated in patient portals?	People/ Tools & Technology	WCAG 2.1; ISO 9241-210; UN DPI Safeguard – Inclusion (Accessibility)
10	Are digital-health dashboards verified for accuracy, timeliness, and completeness of aggregated indicators?	Data	ISSAI 3000-49; ISO 8000; UN DPI Safeguard – Structural Integrity (Accountability)
11	Are grievance redressal and error-correction workflows in place for citizens to contest incorrect health data?	People/ Process	UN CRPD Art. 9; ISSAI 100 Principle A3; UN DPI Safeguard – Safety (Recourse & Redress)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
12	Are algorithms used for triage or predictive diagnosis documented, bias-tested, and approved by competent authorities?	Tools & Technology / Process	<i>OECD AI Principles; ISSAI 130 (Ethics); UN DPI Safeguard – Inclusion (Fairness & Explainability)</i>
13	Are vendor contracts for digital-health platforms including explicit audit-access and data-protection clauses?	Process	<i>ISSAI 4000-17; GUID 5280-7; UN DPI Safeguard – Structural Integrity (Transparency)</i>
14	Is there an incident-response plan for data breaches, including notification timelines and root-cause analysis?	Process/ Data	<i>ISO 27035; ISSAI 3000-52; UN DPI Safeguard – Safety (Security & Trust)</i>
15	Are performance and inclusion metrics (uptime, rural coverage, gender balance) monitored and publicly reported?	People/ Process	<i>ISSAI 3000-36; UN SDG 3 & 10 Indicators; UN DPI Safeguard – Inclusion (Equity & Participation)</i>

EDUCATION

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
1	Is there a national or state-level policy defining governance, ownership, and data-sharing responsibilities for digital-learning platforms?	Process/ Data	<i>ISSAI 4000 Paragraphs 16–18; ISO 27701-7.4; UN DPI Safeguard – Structural Integrity (Governance & Accountability)</i>
2	Are student-identity and credential systems (digital certificates, IDs) securely linked to the DPI identity layer?	Tools & Technology/ Data	<i>ISSAI 3000-38; ISO 29115; UN DPI Safeguard – Safety (Security & Trust)</i>
3	Are e-learning portals accessible to differently-abled learners and low-bandwidth users (WCAG 2.1 compliance)?	People/ Tools & Technology	<i>WCAG 2.1; UN CRPD Art. 9; UN DPI Safeguard – Inclusion (Accessibility)</i>
4	Do authentication and login mechanisms protect minors' privacy and comply with parental-consent laws?	People/ Process	<i>GDPR Art. 8; ISO 27701 Annex B; UN DPI Safeguard – Safety (Privacy & Consent)</i>
5	Are learning-content repositories curated through transparent accreditation and copyright-compliance workflows?	Process	<i>ISSAI 4000– 21; WIPO Copyright Treaty; UN DPI Safeguard – Structural Integrity (Transparency)</i>
6	Are open-source and commercial e-learning systems interoperable through recognised standards (SCORM, LTI, xAPI)?	Tools & Technology/ Process	<i>ISO/ IEC 12785; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability)</i>

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
7	Is there a data-retention policy for student records, assessment data, and digital-credential logs?	Process/ Data	<i>ISO 15489; ISSAI 3000-49; UN DPI Safeguard – Safety (Data Protection)</i>
8	Are examination and assessment platforms equipped with anti-malpractice, proctoring-integrity, and audit-logging controls?	Tools & Technology/ Data	<i>ISO 27001 A.12; GUID 5100 -4.3; UN DPI Safeguard – Safety (Security & Oversight)</i>
9	Are algorithms used for adaptive learning or grading transparent, bias-tested, and periodically validated?	Tools & Technology/ Process	<i>OECD AI Principles; ISSAI 130 (Ethics); UN DPI Safeguard – Inclusion (Fairness & Explainability)</i>
10	Is learner-feedback systematically captured and analysed to improve content quality and inclusivity?	People/ Process	<i>ISSAI 3000-36; ISO 10002; UN DPI Safeguard – Inclusion (Participation)</i>
11	Are teacher and institution performance dashboards validated for data accuracy and fairness of indicators?	Process/ Data	<i>ISO 8000; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Accountability)</i>
12	Are data-sharing agreements between EdTech vendors and education departments subject to independent audit or certification?	Process/ Data	<i>GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Oversight)</i>
13	Do digital-education systems include multilingual interfaces and local-content support to reduce regional inequity?	People/ Tools & Technology	<i>UNESCO Open Education Standards; WCAG 2.1; UN DPI Safeguard – Inclusion (Equity & Access)</i>
14	Are capacity-building and digital-literacy programmes available for teachers, parents, and students to use DPI platforms effectively?	People/ Process	<i>ISSAI 100 Principle A3; UN SDG 4; UN DPI Safeguard – Inclusion (Capacity & Participation)</i>
15	Are continuity and disaster-recovery arrangements (server backups, data replication) tested for e-learning systems?	Tools & Technology/ Data	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Resilience & Sustainability)</i>

AGRICULTURE AND RURAL DEVELOPMENT

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a national digital-agriculture policy defining data ownership, custodianship, and sharing mechanisms between ministries and private agri-tech firms?	Process/ Data	ISSAI 4000 Paragraphs 16–18; ISO 27701-7.4; UN DPI Safeguard – Structural Integrity (Governance & Accountability)
2	Are farmer-registration and beneficiary databases linked to verified identity systems to prevent duplication or ghost entries?	Data/ Process	ISSAI 3000- 38; ISO 8000; UN DPI Safeguard – Structural Integrity (Data Quality & Interoperability)
3	Are Direct Benefit Transfer (DBT) platforms for subsidies and crop insurance integrated with the national payments layer (UPI/ Aadhaar Pay) securely?	Tools & Technology/ Data	GUID 5100-4.3; ISO 27001 A.9; UN DPI Safeguard – Safety (Security & Trust)
4	Do digital-land-records and cadastral systems interface accurately with farmer registries to confirm eligibility for schemes?	Data/ Process	ISSAI 3000- 49; ISO 8000; UN DPI Safeguard – Structural Integrity (Accuracy & Accountability)
5	Are procurement and Minimum Support Price (MSP) platforms transparent and traceable from farmer registration to payment disbursement?	Process/ Data	GUID 5280- 7; ISSAI 4000-21; UN DPI Safeguard – Structural Integrity (Transparency)
6	Are agri-data exchanges governed by open-data standards and anonymisation protocols before sharing with private analytics firms?	Process/ Data	ISO 8000; ISO 27701 Annex B; UN DPI Safeguard – Safety (Privacy & Data Sharing)
7	Are IoT-based sensors and remote-sensing tools used for crop monitoring calibrated, validated, and cyber-secured?	Tools & Technology/ Data	ISO 27017; ISSAI 3000-49; UN DPI Safeguard – Safety (Security & Reliability)
8	Are weather, soil, and market-price datasets verified for accuracy, timeliness, and completeness before being used for decision support?	Data	ISO 8000; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Data Quality)
9	Do farmers have accessible grievance redressal channels (digital/ offline) to contest incorrect subsidy or insurance data?	People/ Process	ISSAI 100 Principle A3; ISO 10002; UN DPI Safeguard – Inclusion (Participation & Redress)
10	Are gender and marginal-farmer inclusion metrics monitored and published for transparency in digital-agriculture initiatives?	People/ Process	UN SDG 2 & 5; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Equity & Representation)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
11	Are vendor contracts for agri-platforms including data analytics and payment intermediaries auditable and compliant with public-procurement norms?	Process	<i>GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Oversight & Accountability)</i>
12	Are APIs connecting agriculture-credit institutions and insurance companies standardised and monitored for uptime data integrity?	Tools & Technology/ Data	<i>W3C API Guidelines; ISO 22301; UN DPI Safeguard – Structural Integrity (Interoperability & Continuity)</i>
13	Are offline and mobile-lite interfaces available for smallholders in low-connectivity regions?	People/ Tools & Technology	<i>WCAG 2.1; UN CRPD Art. 9; UN DPI Safeguard – Inclusion (Accessibility & Equity)</i>
14	Are predictive-analytics models (yield/ price forecasts) validated and free from bias or opaque weighting?	Tools & Technology/ Process	<i>OECD AI Principles; ISSAI (Ethics); UN DPI Safeguard – Inclusion (Fairness & Explainability)</i>
15	Is there a continuity and disaster-recovery plan for agri-data centres to prevent loss of subsidy or crop-insurance records?	Process/ Data	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Resilience & Sustainability)</i>

URBAN GOVERNANCE & SMART CITIES

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
1	Is there an integrated governance framework defining ownership, coordination, and accountability among city departments, utilities, and ICT vendors?	Process/ People	<i>ISSAI 3000-36; GUID 5280-7; UN DPI Safeguard – Structural Integrity (Governance & Accountability)</i>
2	Are smart-city command and control centres operating under defined data-classification and access-control policies?	Tools & Technology/ Data	<i>ISO 27001 A.9; ISSAI 4000-16; UN DPI Safeguard – Safety (Security & Trust)</i>
3	Are geospatial and sensor data collected from IoT devices validated for accuracy and integrity before use in decision-making?	Data/ Tools & Technology	<i>ISO 8000; ISO 27017; UN DPI Safeguard – Structural Integrity (Data Quality & Reliability)</i>
4	Are surveillance and traffic-monitoring systems compliant with privacy and data-protection regulations?	People/ Process	<i>ISO 27701-7.4; GDPR Art. 6; UN DPI Safeguard – Safety (Privacy & Ethical Use)</i>

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
5	Are citizen-service applications (property tax, utilities, grievance redress) accessible and inclusive (WCAG 2.1 compliance)?	People/ Tools & Technology	WCAG 2.1; UN CRPD Art. 9; UN DPI Safeguard – Inclusion (Accessibility & Equity)
6	Are open APIs enabling data exchange between departments (urban planning, utilities, transport) built on common metadata standards?	Tools & Technology/ Data	W3C API Guidelines; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability)
7	Are digital-payment systems for property tax, parking, and utilities secure and reconciled with financial systems?	Process/ Data	ISO 22301; GUID 5100-4.3; UN DPI Safeguard – Safety (Security & Continuity)
8	Is there an incident-response mechanism for cyberattacks or data breaches in smart-city platforms?	Process/ Data	ISO 27035; ISO 22301; UN DPI Safeguard – Safety (Resilience & Trust)
9	Are smart-meter and billing systems tested for fairness, accuracy, and error-handling (automated vs. manual reconciliation)?	Tools & Technology/ Data	ISO 8000; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Accountability & Transparency)
10	Do city dashboards disclose real-time performance indicators (air quality, waste management, energy use) with public access?	People/ Process	OECD Open Data Charter; ISSAI 3000-49; UN DPI Safeguard – Inclusion (Transparency & Participation)
11	Are procurement contracts for digital infrastructure transparent, competitive, and include audit-access clauses?	Process	GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Procurement & Oversight)
12	Are citizen feedback and complaint logs integrated into periodic service-level performance reviews?	People/ Process	ISO 10002; ISSAI 100 Principle A3; UN DPI Safeguard – Inclusion (Feedback & Redress)
13	Are interoperability standards between GIS, IoT, and ERP systems documented and periodically updated?	Tools & Technology/ Data	ISO 19115; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability & Sustainability)
14	Are environmental and disaster-management modules integrated into the smart-city platform for early warning and response?	Process/ Tools & Technology	ISO 22301; UN SDG 11; UN DPI Safeguard – Safety (Resilience & Public Protection)
15	Are digital-literacy and capacity-building programmes conducted for municipal employees and citizens to use smart-city services effectively?	People/ Process	ISSAI 100 Principle A3; UN SDG 4; UN DPI Safeguard – Inclusion (Capacity & Empowerment)

E- COMMERCE & MSME ENABLEMENT

This domain is critical because open digital-commerce networks (like ONDC or Beckn-based platforms) sit squarely on DPI's payments, identity, and data-exchange layers. They test transparency, neutrality, and fairness in algorithmic marketplaces which are rich ground for both compliance and performance audits.

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a clear policy framework defining roles, accountability, and dispute-resolution for open digital-commerce networks?	Process/ People	ISSAI 3000-36; ISSAI 4000 Paragraphs 16–18; UN DPI Safeguard – Structural Integrity (Governance & Accountability)
2	Are onboarding processes for sellers and buyers transparent, non-discriminatory, and logged for audit?	Process/ Data	OECD Competition Principles; GUID 5280-7; UN DPI Safeguard – Inclusion (Fair Access & Transparency)
3	Are merchant and MSME identities verified through trusted digital-ID and KYC mechanisms?	People/ Data	ISO 29115; ISSAI 3000-38; UN DPI Safeguard – Safety (Authentication & Trust)
4	Are product-catalogue and pricing algorithms auditable for fairness, ranking bias, and transparency?	Tools & Technology/ Process	OECD AI Principles; ISSAI 130 (Ethics); UN DPI Safeguard – Inclusion (Fairness & Explainability)
5	Are digital-payment gateways integrated securely with national DPI layers (UPI/ RuPay/ Aadhaar Pay) and compliant with anti-fraud norms?	Tools & Technology/ Data	ISO 27001 A.9; GUID 5100-4.3; UN DPI Safeguard – Safety (Security & Resilience)
6	Are transaction logs, refunds, and charge-back processes fully traceable and reconcilable?	Process/ Data	ISO 22301; ISSAI 4000-21; UN DPI Safeguard – Structural Integrity (Transparency & Auditability)
7	Are MSME participants provided equal access to APIs, documentation, and testing sandboxes?	People/ Tools & Technology	OECD Open Markets; ISSAI 100 Principle A3; UN DPI Safeguard – Inclusion (Equity & Participation)
8	Are consumer-data-sharing consents explicit, time-bound, and revocable?	Process/ Data	GDPR Art. 7; ISO 27701 Annex B; UN DPI Safeguard – Safety (Privacy & Consent)
9	Are grievance redressal portals functional, multilingual, and monitored for turnaround time?	People/ Process	ISO 10002; UN SDG 9; UN DPI Safeguard – Inclusion (Feedback & Redress)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
10	Are vendor-rating and reputation systems protected from manipulation and fake reviews?	Tools & Technology/ Process	<i>OECD Digital Economy Guidelines; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Integrity & Accountability)</i>
11	Are data-exchange protocols between buyer, seller, and logistics entities built on open standards (Beckn/ REST/ W3C)?	Tools & Technology/ Data	<i>W3C API Guidelines; ISO 8000; UN DPI Safeguard – Structural Integrity (Interoperability & Openness)</i>
12	Are logistics-tracking and fulfilment data retained and auditable for last-mile delivery verification?	Data/ Process	<i>ISO 15489; GUID 5100-4.3; UN DPI Safeguard – Safety (Traceability & Accountability)</i>
13	Are financial-settlement systems subject to independent certification for reconciliation accuracy and timeliness?	Process/ Data	<i>ISSAI 4000-21; ISO 22301; UN DPI Safeguard – Structural Integrity (Resilience & Oversight)</i>
14	Are platform operators required to publish transparency reports on access, suspension, or delisting actions?	Process/ People	<i>OECD Digital Transparency Principles; ISSAI 100; UN DPI Safeguard – Inclusion (Transparency & Rights Awareness)</i>
15	Are digital-literacy and onboarding-assistance programmes provided for small retailers, women entrepreneurs, and rural MSMEs?	People/ Process	<i>UN SDG 5 & 8; ISSAI 100 Principle A3; UN DPI Safeguard – Inclusion (Capacity & Empowerment)</i>

LAND AND PROPERTY REGISTRIES

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
1	Is there a clear legal and policy framework defining ownership, custodianship, and public access to digital land records and cadastral maps?	Process/ People	ISSAI 4000 Paragraphs 16–18; ISO 15489; UN DPI Safeguard – Structural Integrity (Governance & Accountability)
2	Are landholder identities verified against trusted digital-ID systems during registration, mutation, and transfer processes?	People/ Data	ISSAI 3000-38; ISO 29115; UN DPI Safeguard – Safety (Authentication & Trust)
3	Is the end-to-end property registration workflow (search → valuation → stamp duty → registration → mutation) digitised with auditable checkpoints?	Process/ Tools & Technology	GUID 5100-4.3; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Process Transparency)
4	Are cadastral maps and textual records synchronised (spatial-textual concordance) with version control and change logs?	Data/ Tools & Technology	ISO 19115; ISO 8000; UN DPI Safeguard – Structural Integrity (Data Accuracy & Reliability)
5	Are APIs for inter-agency data exchange (revenue, urban planning, utilities, courts, banks) standardised and access-controlled?	Tools & Technology/ Data	W3C API Guidelines; ISO 27001 A.9; UN DPI Safeguard – Structural Integrity (Interoperability & Security)
6	Are valuation engines and circle-rate calculators transparent, reproducible, and periodically validated against market data?	Tools & Technology/ Process	ISSAI 3000-49; OECD Good Practices; UN DPI Safeguard – Inclusion (Fairness & Transparency)
7	Do digital-payment and e-stamp systems reconcile completely with treasury ledgers, with automated exception handling?	Process/ Data	ISO 22301; ISSAI 4000-21; UN DPI Safeguard – Structural Integrity (Resilience & Accountability)
8	Are chain-of-title histories and encumbrance records complete, time-stamped, and tamper-evident?	Data	ISO 15489; GUID 5100-4.3; UN DPI Safeguard – Safety (Integrity & Non-Repudiation)
9	Are privacy safeguards applied to sensitive owner data while ensuring legitimate public access (searchability vs. redaction)?	Process/ Data	ISO 27701; GDPR Principles; UN DPI Safeguard – Safety (Privacy & Proportionality)
10	Are offline/ assisted channels available for citizens in low-connectivity areas, with parity of service and fees?	People/ Process	WCAG 2.1 (Usability); ISSAI 100 (Equity); UN DPI Safeguard – Inclusion (Accessibility & Fair Access)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference / Criteria
11	Are grievance redressal and dispute-resolution workflows integrated (objections, appeals, court orders) with audit trails?	People/ Process	<i>ISO 10002; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Redress & Accountability)</i>
12	Are bulk data exports and third-party access governed by licensing, anonymisation, and rate-limiting to prevent misuse?	Process/ Data	<i>OECD Open Data Principles; ISO 27701; UN DPI Safeguard – Safety (Data Sharing & Protection)</i>
13	Are geo-spatial inputs (survey, drone/ RS) calibrated, quality-checked, and linked to ground control points?	Tools & Technology/ Data	<i>ISO 19157 (Data Quality); ISO 8000; UN DPI Safeguard – Structural Integrity (Data Accuracy & Reliability)</i>
14	Are business-continuity and disaster-recovery plans tested for registries (RPO/RTO, backups, cold/ warm sites)?	Process/ Tools & Technology	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Continuity & Sustainability)</i>
15	Do procurement/ contracts for registry platforms include open-standards, portability, and explicit audit-access clauses?	Process	<i>GUID 5280-7; ISSAI 4000-17; UN DPI Safeguard – Structural Integrity (Procurement & Oversight)</i>

PUBLIC PROCUREMENT & SUPPLY CHAINS

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a national e-procurement policy that clearly defines digital workflow, roles, and responsibilities of buyers, bidders, and auditors?	Process/ People	<i>GUID 5280-3; ISSAI 4000 Paragraphs 16–18; UN DPI Safeguard – Structural Integrity (Governance & Accountability)</i>
2	Are tender documents, corrigenda, and bid submissions published digitally in a transparent, time-stamped manner?	Process/ Data	<i>ISSAI 4000-21; OECD Procurement Principles; UN DPI Safeguard – Inclusion (Transparency & Access)</i>
3	Are vendor registrations and empanelments linked to verified digital identities and KYC data to prevent duplication or fraud?	People/ Data	<i>ISO 29115; ISSAI 3000-38; UN DPI Safeguard – Safety (Authentication & Trust)</i>
4	Are bid-evaluation algorithms and auto-scoring modules transparent, version-controlled, and auditable?	Tools & Technology/ Process	<i>OECD AI Principles; GUID 5100-4.3; UN DPI Safeguard – Inclusion (Fairness & Explainability)</i>
5	Are bid openings digitally witnessed and time-stamped to maintain non-repudiation and fairness?	Tools & Technology/ Data	<i>ISSAI 4000-21; ISO 27001 A.9; UN DPI Safeguard – Safety (Integrity & Security)</i>
6	Are contract-award decisions and evaluation criteria published with explanatory notes for public scrutiny?	People/ Process	<i>OECD Integrity Framework; ISSAI 100; UN DPI Safeguard – Inclusion (Transparency & Accountability)</i>
7	Are procurement portals interoperable with finance, inventory, and audit systems for end-to-end traceability?	Tools & Technology/ Data	<i>ISO 8000; GUID 5280-4.2; UN DPI Safeguard – Structural Integrity (Interoperability & Oversight)</i>
8	Are contract management and payment modules linked to the national payment rail and subject to reconciliation controls?	Process / Data	<i>ISSAI 4000-21; ISO 22301; UN DPI Safeguard – Structural Integrity (Resilience & Accountability)</i>
9	Do e-tendering systems include fraud-detection and red-flag analytics for bid collusion or cartel behaviour?	Tools & Technology/ Process	<i>OECD Anti-Cartel Guidelines; ISSAI 130 (Ethics); UN DPI Safeguard – Safety (Integrity & Risk Management)</i>

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
10	Are supplier-performance ratings captured and published to promote accountability and competition?	Process/ People	<i>Procurement Transparency; ISSAI 3000-36; UN DPI Safeguard – Inclusion (Equity & Participation)</i>
11	Are supply-chain tracking modules (warehousing, distribution, delivery) integrated with digital ledgers and GPS validation?	Tools & Technology/ Data	<i>ISO 28000; GUID 5100-4.3; UN DPI Safeguard – Structural Integrity (Traceability & Reliability)</i>
12	Are change-orders, extensions, and price variations digitally logged with approval hierarchies and audit trail?	Process/ Data	<i>ISSAI 4000-21; ISO 15489; UN DPI Safeguard – Structural Integrity (Auditability & Documentation)</i>
13	Are green procurement criteria (environmental sustainability) integrated into tender evaluation and reporting?	Process/ People	<i>UN SDG 12; OECD Green Procurement Guidelines; UN DPI Safeguard – Structural Integrity (Sustainability)</i>
14	Are dispute-resolution and arbitration records maintained digitally and analysed for recurring risks?	Process/ Data	<i>ISSAI 3000-49; ISO 8000; UN DPI Safeguard – Structural Integrity (Redress & Learning)</i>
15	Are procurement-system logs subject to periodic independent IT audit for security, availability, and integrity?	Tools & Technology/ Data	<i>GUID 5100-3.2; ISO 27040; UN DPI Safeguard – Safety (Security & Assurance)</i>

TAXATION & FINANCIAL MANAGEMENT

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
1	Is there a unified digital-taxation and financial-management policy defining roles, responsibilities, and interoperability between revenue and expenditure systems?	Process/ People	ISSAI 4000 Paragraphs 16–18; GUID 5100-3.2; UN DPI Safeguard – Structural Integrity (Governance & Accountability)
2	Are taxpayer-identification numbers and entity profiles linked securely to national digital-ID and business-registry databases?	Data/ Process	ISO 29115; ISSAI 3000-38; UN DPI Safeguard – Safety (Authentication & Trust)
3	Are e-invoicing and return-filing platforms designed for data-accuracy, validation, and real-time reconciliation?	Tools & Technology/ Data	ISO 8000; ISSAI 3000-49; UN DPI Safeguard – Structural Integrity (Data Quality & Reliability)
4	Are transaction logs for Goods and Services Taxes, customs, or Income-tax systems immutable, time-stamped, and stored with adequate retention and backup?	Data/ Tools & Technology	ISO 15489; ISO 27040; UN DPI Safeguard – Safety (Integrity & Resilience)
5	Are risk-profiling and analytics algorithms (fraud detection, anomaly scoring) transparent, validated, and periodically recalibrated?	Tools & Technology/ Process	OECD AI Principles; ISSAI 130 (Ethics); UN DPI Safeguard – Inclusion (Fairness & Explainability)
6	Are taxpayer data protected through encryption at rest and in transit, with clear segregation of duties for administrators?	Tools & Technology/ Data	ISO 27001 A.9; ISO 27701-7.4; UN DPI Safeguard – Safety (Data Protection & Privacy)
7	Are refunds, rebates, and input-credit claims processed automatically with traceable audit trails and exception handling?	Process/ Data	ISSAI 4000-21; ISO 22301; UN DPI Safeguard – Structural Integrity (Accountability & Transparency)
8	Are integration points between tax systems and national-payment gateways secured and reconciled daily?	Tools & Technology/ Data	GUID 5100-4.3; ISO 27017; UN DPI Safeguard – Safety (Security & Trust)
9	Are APIs used by accounting software, fintechs, and auditors standardised, rate-limited, and logged for usage monitoring?	Tools & Technology/ Data	W3C API Guidelines; ISO 22301; UN DPI Safeguard – Structural Integrity (Interoperability & Oversight)
10	Are financial-management-information systems (FMIS) providing real-time dashboards on receipts, expenditures, and balances to decision-makers?	Process/ Tools & Technology	ISSAI 3000-49; OECD Open Budget Standards; UN DPI Safeguard – Inclusion (Transparency & Public Value)

No.	Illustrative Audit Question	Primary Audit Dimension (PPT/ Data)	Reference/ Criteria
11	Are audit trails for budget re-appropriations, supplementary grants, and re-leases maintained digitally and version-controlled?	Process/ Data	<i>ISO 15489; ISSAI 4000-21; UN DPI Safeguard – Structural Integrity (Auditability & Documentation)</i>
12	Are internal-control modules (commitment control, approval workflows) configured to prevent unauthorised spending?	Process/ Tools & Technology	<i>ISSAI 4000-17; ISO 22301; UN DPI Safeguard – Structural Integrity (Control & Compliance)</i>
13	Are tax-appeals, grievance redressal, and compliance-monitoring systems integrated and publicly trackable?	People/ Process	<i>ISO 10002; ISSAI 100 Principle A3; UN DPI Safeguard – Inclusion (Access & Redress)</i>
14	Are capacity-building programmes conducted for tax officers and financial managers to use data-analytics dashboards effectively?	People/ Process	<i>UN SDG 16; ISSAI 100 Principle A3; UN DPI Safeguard – Inclusion (Capacity & Participation)</i>
15	Is a business-continuity and disaster-recovery plan implemented for tax and treasury data centres with tested RTO/ RPO targets?	Process/ Data	<i>ISO 22301; ISO 27040; UN DPI Safeguard – Structural Integrity (Resilience & Sustainability)</i>

The sectoral audit questions presented in this annexure are intended to serve as **illustrative reference points** for Supreme Audit Institutions (SAIs) when planning or conducting audits of Digital Public Infrastructure (DPI)-enabled programmes. They reflect the diversity of public-sector contexts in which DPI operates, from social welfare and health to taxation and urban governance and highlight the audit dimensions that are most critical for transparency, efficiency, and inclusion.

These questions should be viewed as **modular building blocks** rather than a fixed checklist. Each SAI is encouraged to adapt them according to:

1. National priorities and legal mandates, particularly regarding access to data and private-sector entities;
2. Sectoral maturity, as DPI adoption level vary widely across domains;
3. **Available evidence sources**, including administrative data, APIs, user surveys, or physical verification; and
4. **Audit objectives**, as defined through the Audit Design Matrix (ADM) in **Chapter 7**.

Auditors may also integrate sectoral questions across domains where DPI components overlap for instance, combining **Digital Identity and Payments** in welfare audits or **Data Exchange** in health and education audits.

When used systematically, these sectoral frameworks enable SAIs to conduct audits that are:

- **Risk-based**, prioritising high-value or high-vulnerability areas;
- **Standards-aligned**, consistent with ISSAI 3000 (Performance Audit), ISSAI 4000 (Compliance Audit), and GUID 5100 (Information Systems Audit); and
- **Outcome-oriented**, linking system design to citizen value and accountability.

Ultimately, these questions aim to help SAIs assess whether the digital transformation of public services truly advances **economy, efficiency, effectiveness, equity, and ethical integrity**, the core principles of DPI audit.

Notes

[illegible]



**COMPTROLLER AND
AUDITOR GENERAL OF INDIA**

<http://www.cag.gov.in>