

DIGITAL READINESS TOOLKIT FOR NATIONAL HUMAN RIGHTS INSTITUTIONS



Supported by

 **Norway**

Copyright © **UNDP 2026**. All rights reserved.

One United Nations Plaza, NEW YORK, NY10017, USA

The **United Nations Development Programme (UNDP)** is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at [@UNDP](https://twitter.com/UNDP).

The views expressed in this publication do not necessarily represent those of the member countries of the UNDP Executive Board or of those institutions of the United Nations system that are mentioned herein.

The designations and terminology employed, and the presentation of material, do not imply any expression or opinion whatsoever on the part of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or of its frontiers or boundaries.

Cover photo ©World Bank Tonga

The Digital Readiness Toolkit for National Human Rights Institutions (NHRIs) was developed through the collaborative efforts of the United Nations Development Programme (UNDP), the Office of the United Nations High Commissioner for Human Rights (OHCHR), and the Global Alliance of National Human Rights Institutions (GANHRI) under the longstanding Tripartite Partnership to support National Human Rights Institutions. The development of this Toolkit was made possible through the generous support of the Government of Norway through UNDP's Global Programme for Strengthening the Rule of Law, Human Rights, Justice and Security for Sustainable Peace and Development, Phase IV.

The report was co-authored by (alphabetically) Justin Nettman and Roqaya Dhaif, Policy Specialist with substantive contributions from Julie Vandassen, Human Rights Policy Specialist. The toolkit was completed under the overall guidance and support of Sarah Rattray, Global Lead for Human Rights at UNDP.

This toolkit has benefited significantly from the guidance and expertise of a Reference Group composed of representatives from national human rights institutions (NHRIs) across different regions. Their practical insights, institutional experience, and engagement throughout the process helped ensure that the guidance reflects the diverse contexts in which NHRIs operate. In particular, sincere appreciation is extended to the NHRIs of Palestine, Nigeria, Oman, Nepal, Uruguay, Honduras, and Malawi.

NHRIs play a vital role in promoting and protecting human rights. In an increasingly digital world, the environments in which NHRIs operate are evolving rapidly. Human rights violations are documented, communicated, and sometimes perpetrated through digital means, while populations increasingly expect institutions to provide accessible, secure, and responsive digital services. For NHRIs, strengthening digital readiness is therefore no longer optional, it is an essential component of institutional effectiveness and resilience.

Digital technologies offer important opportunities for NHRIs to enhance their work. Evidence from institutions and world shows that secure digital systems can improve complaint intake and case management, strengthen evidence collection, facilitate collaboration with other public institutions, and enable better monitoring of human rights trends. When designed and implemented responsibly, digital tools can expand access to justice, improve transparency, and support evidence-based policy engagement. At the same time, digitalization presents significant challenges. NHRIs can handle highly sensitive information concerning victims, witnesses, and human rights defenders. Weak digital systems can expose individuals to serious risks, including privacy breaches, surveillance, or retaliation. In addition, digital transformation requires careful attention to governance, sustainability, legal compliance, and institutional capacity. Technology alone does not strengthen institutions, it must be accompanied by strong processes, skilled people, and rights-based safeguards.

The Digital Readiness Toolkit has been developed to support NHRIs in navigating this digital transformation. The toolkit provides practical guidance for assessing digital maturity, identifying readiness gaps, and planning the safe and effective adoption of digital systems. It offers a structured approach that integrates technology with institutional governance, legal frameworks, operational processes, and human rights principles. Importantly, this toolkit recognizes that NHRIs operate in diverse national contexts with varying levels of resources, infrastructure, and technical capacity. Digital transformation is not a one-size-fits-all process. By placing human rights principles at the centre of digital transformation, NHRIs can ensure that technology serves the public interest and enhances their ability to promote and protect human rights in an increasingly digital world.



Amina Bouayach

Chairperson
Global Alliance for National Human
Rights Institutions (GANHRI)

A handwritten signature in black ink that reads "Amina Bouayach". The signature is written in a cursive, flowing style.

ACKNOWLEDGEMENTS	3
FOREWORD	4
GLOSSARY	7
PART 1 INTRODUCTORY GUIDANCE	11
1. Introduction	12
2. Conceptual Framework for NHRI Digital Transformation	14
2.1 Integrating Digital Readiness into NHRI Capacity Assessment	14
2.2 The Importance of Digitization for NHRIs	15
2.3 Risks and barriers of Digitization for NHRIs	16
3. Case examples: NHRI Digital Strategy and Systems Comparisons	21
PART 2 DIGITAL MATURITY & DIGITAL READINESS CHECKLISTS	29
1. Digital maturity assessment	30
1.1 Digital Maturity Level Index	31
1.2 Maturity and Capability Progression Framework	33
2. Introduction to the Digital Readiness Checklist	35
2.1 Step 1: Digital Prerequisites Screening Tool	36
2.2 Step 2: Choosing the Appropriate Assessment Approach	38
3. STEP 3: NHRI Digital Readiness Self-Assessment checklists	40
3.1 People – Skills, Roles, and Leadership	41
3.2 Processes – Planning, Governance, and Project Management	43
3.3 Governance – Legal and Policy Framework	45
3.4 Technology – technical requirements for a safe and secure system	48
3.5 Finances	63
PART 3 DIGITAL SOLUTIONS FOR NHRIS	66
1. Overview of Solution Pathways	67
Solution Pathway A Off-the-shelf solutions	68
Solution Pathway B Internally developed / bespoke systems	69
Solution Pathway C Hybrid solutions	70
2. Technical requirements based on the solution pathway	71
2.1 Off-the-shelf NHRI system	71
A. What it requires	71
B. Risks and Mitigation of off-the-shelf systems	72
2.2 Internally developed bespoke NHRI system (open source)	73
A. What it requires	73
B. Risks and Mitigation of inhouse developed bespoke systems	74

3. AI in NHRI Systems	75
4. Aligning Solutions with National Digital Initiatives	77
5. Conclusion and Next Steps	77

ANNEX 1**79**

1. Digital Technology (Cloud vs On Premises)	80
2. ICT Best Practices (Governance, Sustainability and Delivery)	82
2.1. ICT Maintenance	82
2.2. ICT Governance and frameworks	83
3. Important key ICT principles	84
4. Digital Sustainability and Capacity Building	84
5. Recommendations for Implementation of digital services in NHRIs	84
6. ICT Project Management for NHRI Digitalization	85
7. Essential templates and policies	85
7.1. Requirement templates	86
7.2. Core ICT Policies for NHRIs	86

ANNEX 2**87**

1. NHRI Toolkit Companion Resources Repository	88
1.1 ICT Governance and Service Management Resources	88
1.2 Project, Design, and Assessment Resources	90

AES	Advanced Encryption Standard
API	Application Programming Interface
APM	Application Performance Monitoring
AI	Artificial Intelligence
AWS	Amazon Web Services
AXELOS	AXELOS Limited (owner of ITIL® and PRINCE2®)
BI	Business Intelligence
BRS	Business Requirements Specification
CAB	Change Advisory Board
CAPEX	Capital Expenditure
CCTA	Central Computer and Telecommunications Agency
COBIT	Control Objectives for Information and Related Technologies
CRM	Client Relationship Management
DEV	Development (Reference to technology)
DRT	Digital Readiness Toolkit
DR	Disaster Recovery
DTMLI	Digital Transformation Maturity Level Index
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSAR's	Data Subject Access Requests
ECC	Elliptic-Curve Cryptography
EDR	Endpoint Detection & Response
ESB	Enterprise Service Bus
ETL	Extract Transform Load (Data integration layer)
FOI	Freedom of Information
FRS	Functional Requirements Specification
GDPR	General Data Protection Regulation
HP	Hewlett-Packard

HQ	Headquarters
HRD	Human Rights Defenders
HRIA	Human Rights Impact Assessment
HRAT	Human Rights Abuse Tracker
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HTTP	Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IBM	International Business Machines
ICT	Information and Communications Technology
ID	Identifier / Identity Document
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KMS	Key Management Service
KPI	Key Performance Indicator
LLM	Modern Language Models
MDA	Ministries, Departments & Agencies
MDM	Master Data Management
MFA	Multi-Factor Authentication
M&E	Monitoring & Evaluation
NAS	Network-Attached Storage
NDPR	Nigeria Data Protection Regulation
NFR	Non-Functional Requirements
NHRC	National Human Rights Commission (Nigeria)
NHRI	National Human Rights Institutions
NIST	National Institute of Standards and Technology

NPM	National Prevention Mechanism
OIDC	OpenID Connect (login/authentication standard)
OPEX	Operating Expenditure
OTS	Off-the-shelf
OPCAT	Optional Protocol to the Convention Against Torture
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PMO	Project Management Office
POPIA	Protection of Personal Information Act (South Africa)
PoC	Proof of Concept
RACI	Responsible, Accountable, Consulted, Informed
RAID	Redundant array of independent disks
RBAC	Role-Based Access Control
RFP	Request for Proposal
REST	Representational State Transfer
RoPA	Record of Processing Activities
SAHRC	South African Human Rights Commission
SaaS	Software as a Service
SAML	Security Assertion Markup Language (federated login standard)
SAN	Storage Area Network
SCC	Standard Contractual Clauses
SDLC	Software Development Life Cycle
SGBV	Sexual and Gender-Based Violence
SIEM	Security Information & Event Management
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SOP	Standard Operating Procedures
SMS	Short Message Service
SRE	Site Reliability Engineering
SSL	Secure Sockets Layer

SSO	Single Sign-On
SLO	Service Level Objective
TLS	Transport Layer Security
TCO	Total Cost of Ownership
TOGAF	The Open Group Architecture Framework
UAT	User Acceptance Testing
UBAC	User Based Access Control
UI	User Interface
UK	United Kingdom
UNDP	United Nations Development Program
USSD	Unstructured Supplementary Service Data
UPS	Uninterruptible Power Supply
UPR	Universal Periodic Review
UX	User Experience
VPN	Virtual Private Network
WCAG 2.1 AA	Web Content Accessibility Guidelines
VPN	Virtual Private Network
XDR	Extended Detection & Response

Part 1

INTRODUCTORY GUIDANCE

Objectives of the Toolkit

Digital transformation is increasingly essential for strengthening the effectiveness, resilience, and accountability of NHRIs. While not all NHRI functions can or should be digitalised, carefully designed digital systems can enhance data management, coordination, and service delivery. Applying a Human Rights–Based Approach (HRBA), this **NHRI Digital Readiness Toolkit** supports institutions in identifying where digital tools add value while ensuring that digitalisation upholds human dignity, protects individuals' rights, and reinforces the core principles of participation, inclusion, equality, transparency, and accountability. The toolkit empowers institutions to modernize operations so they can serve their mandates with faster speed and more precision. Ultimately, digital transformation should serve one purpose above all others; strengthening the ability of NHRIs to protect and promote human rights for all.

The Digital Readiness Toolkit aims to:

- ↳ Provide a **practical structured, step-by-step guide** for assessing, planning, implementing, and maintaining digital systems that support the core functions of NHRIs, taking into account institutional context, mandates and resource levels.
- ↳ Support **evidence-based decision-making** through a readiness checklist, comparison tables of different systems, good governance models and implementation roadmaps.
- ↳ Promote **standardization and interoperability**, drawing on international best practices and successful NHRI case studies.
- ↳ Embed human rights principles, including **principles of data protection, transparency, and accountability** across all digital system components, ensuring that technology serves rights holders safely and ethically.
- ↳ Encourage **self-assessment** and iterative development, ensuring systems match the NHRI's evolving needs and capacity and emerging technologies.
- ↳ Ensure compliance with national **data protection laws and regulations**, safeguarding individual privacy.
- ↳ Acknowledge and mitigate digital risks.

Digital readiness is not a uniform or fixed condition across NHRIs. A meaningful assessment must take into account the institutional, legal, financial, and infrastructural realities in which an NHRI operates. In low resourced or digitally fragmented contexts, foundational conditions such as stable leadership support, basic ICT capacity, connectivity, power supply, budget availability, and basic governance controls may be absent or minimal. Digital readiness is not just about the availability of technology, but also about the institution's ability to plan, manage, and sustain digital transformation over sustained periods of time without donor intervention or support.

Digital readiness should therefore be understood as context specific and conditional. The purpose of this assessment is not only to measure preparedness for new digital systems, but also to identify the enabling conditions and sequencing steps required to make digital transformation feasible, safe, and actionable.

This Digital Readiness Toolkit is not intended to prescribe which specific systems NHRIs should digitalise, nor does it mandate particular ICT standards, technologies, or implementation frameworks. Each NHRI operates within its own national, legal and institutional context, and decisions regarding system design, technology selection, and implementation sequencing must remain with the NHRI itself.

Instead, the toolkit provides guidance on key institutional, governance, and technical considerations that support effective digital development. It is intended to help NHRIs approach digital transformation in a structured and strategic manner, ensuring that any technological investments are introduced in ways that are controlled, secure, efficient, and sustainable.

Recognising that digital technologies and standards evolve rapidly, the toolkit is intentionally designed to remain flexible and adaptable as new technologies, approaches, and institutional needs emerge. By focusing on readiness, principles, and institutional capability, it aims to support NHRIs in strengthening their ability to adopt digital systems that improve service delivery, enhance operational efficiency, and uphold the protection of human rights. In doing so, the toolkit serves as a practical guide to help institutions maximise the benefits of digital transformation while maintaining strong governance, accountability, and security standards.

Who is the Toolkit for

This Digital Readiness Toolkit is designed to support NHRIs at **all stages** of digital development, from those beginning their digital journey to those with advanced systems in place. It is tailored for the following stakeholders:

- ↳ **Leadership and strategic planners:** to help align digital systems with institutional mandates and digital national priorities.
- ↳ **IT Teams:** to guide those responsible for designing and implementing technology programs or solutions.
- ↳ **Legal and compliance officers:** to ensure adherence to data protection, data privacy, and governance frameworks.
- ↳ **Donors, strategic, and technical partners:** to support institutional growth through financing, technical assistance, data governance collaboration, interoperability planning, and the development of rights-based digital ecosystems.
- ↳ **Monitoring and evaluation teams:** to assist in tracking human rights indicators and assessing institutional performance more effectively.

How to Use the Toolkit

The toolkit is modular and adaptable, allowing NHRIs to tailor its use to their specific digital needs. The toolkit supports NHRI in the following areas:

- ↳ **Self-Assessment:** digital maturity Checklists to evaluate NHRIs' current digital capacity and identify readiness gaps.
- ↳ **System planning:** guidance on technical specifications, and cost estimates to define a suitable digital strategy.
- ↳ **Stakeholder engagement:** technical information to facilitate discussions with internal and external stakeholders, including legal teams, data protection officers, and donor partners.
- ↳ **Stakeholder engagement:** technical information to facilitate discussions with internal and external stakeholders, including legal teams, data protection officers, donor partners, National Institutes of Statistics, and other strategic or technical institutions involved in data governance and digital public infrastructure.
- ↳ **Procurement and implementation:** templates and guidelines which assist in the documentation, selection, and procurement of the right systems securely and transparently.
- ↳ **Monitoring and review:** built-in indicators to track progress and streamline reporting for audits or donors.

2. CONCEPTUAL FRAMEWORK FOR NHRI DIGITAL TRANSFORMATION

Digital transformation should be viewed as an integral component of institutional capacity development, rather than as a stand-alone technical or Information and Communications Technology (ICT) upgrade. For NHRIs, digital readiness influences how effectively they fulfil their mandate to protect, promote, and monitor human rights, address emerging challenges, and engage effectively with stakeholders. NHRIs may wish to consider digital transformation alongside broader institutional development priorities identified through tools such as the NHRI Capacity Assessment.

2.1 INTEGRATING DIGITAL READINESS INTO NHRI CAPACITY ASSESSMENT

The [NHRI Capacity Assessment Guidance](#)¹ outlines a process of self-assessment assisted by external expert facilitators and provides a step-by-step approach to identifying specific organizational challenges. The assessment methodology incorporates both qualitative and quantitative elements in assessing the current situation of the NHRI, identifying weaknesses, and forecasting future capacity requirements. Moreover, the [Global Principles](#)² for the [Capacity Assessment of NHRIs](#) outline the common success factors in Capacity Assessments. Capacity assessments are designed to identify existing capacities and those needed for an NHRI to fulfil its mandate effectively, with due regard to relevant human rights norms and standards.

Digital readiness can be considered as a cross-cutting and complementary dimension within this methodology. Rather than focusing narrowly on ICT infrastructure, this approach assesses the extent to which digital systems, processes, and capabilities enable and strengthen the NHRI's core functions and institutional performance.

Embedding digital readiness within the NHRI capacity assessment allows the process to:

- ↳ **Identify how digital systems and processes support NHRI's core functions** (e.g., complaints management, investigations, monitoring and reporting, public outreach, detention monitoring, advisory and legislative engagement, follow-up on recommendations).
- ↳ **Assess digital gaps and vulnerabilities** such as cybersecurity, data protection, privacy, and digital accessibility.
- ↳ **Develop actionable recommendations** that align with the NHRI's strategic objectives and operational context, and human rights obligations.
- ↳ **Foster organizational learning and adaptation** by integrating digital considerations into planning, resource allocation, and institutional development cycles.

By broadening the scope of capacity assessments to explicitly include digital readiness, NHRIs can gain a more holistic understanding of institutional capacities and be better equipped to integrate digital transformation into long-term planning and implementation.

1 Office of the United Nations High Commissioner for Human Rights, 'Capacity Assessment Manual for National Human Rights Institutions', United Nations Development Programme and Asia Pacific Forum of National Human Rights Institutions, United Nations, 2011.

2 United Nations Development Programme, 'Global Principles for Capacity Assessment of National Human Rights Institutions', 2016.

2.2 THE IMPORTANCE OF DIGITIZATION FOR NHRIS

Digital readiness offers important opportunities for NHRIs to enhance their work. Evidence from institutions shows that secure digital systems can improve complaint intake and case management, strengthen evidence collection, facilitate collaboration with other public institutions, and enable better monitoring of human rights trends. When designed and implemented responsibly, digital tools can expand access to justice, improve transparency, and support evidence-based policy engagement.

1. PROTECTING INSTITUTIONS, DEFENDERS, AND COMPLAINANTS

Secure digital systems enhance the protection of sensitive data and thus safeguard human rights defenders and complainants. A secure system with features such as multi-factor authentication (MFA), encrypted platforms would reduce the risks of unwanted tampering, unauthorized access, and the loss of critical data.

2. STRENGTHENING ACCOUNTABILITY AND TRANSPARENCY

Digital workflows improve governance through role-based access control (RBAC), automation, and immutable audit trails. These tools support both internal oversight and external accountability mechanisms.

3. ENHANCING OPERATIONAL EFFICIENCY

Automating routine tasks, such as deadline reminders, status updates, and data extraction, reduces administrative bottlenecks. This frees up staff for high-value work like advocacy and policy engagement, which is vital for resource-constrained NHRIs.

4. FOSTERING COLLABORATION AND INTEROPERABILITY

Digital systems enable NHRIs to work more effectively with other public institutions and partners, allowing for secure information-sharing, compatible data formats, and where appropriate, connections with national justice, civil registration, or identity systems. This strengthens the NHRI's contribution to cross-cutting efforts such as transitional justice, anti-corruption, and gender equality.

By adopting interoperable systems, NHRIs are better positioned to engage on equal footing with ministries, courts, and civil society organizations, and to participate meaningfully in coordinated governance responses.

2.3 RISKS AND BARRIERS OF DIGITIZATION FOR NHRIS

Digitization not only expands access to services such as complainants via online intaking, remote investigation data inputting and access to digital findings, it also introduces rights, security, governance, and overall sustainability. Global guidance emphasizes that technology must be deployed in ways that protect human rights, not just internal efficiency.³

For an NHRI it means using secure, interoperable systems to receive complaints, manage cases, store evidence, coordinate referrals, document human rights violations, and publish findings. When done well, digitization improves continuity of work and reach (via web, mobile, SMS, call center), supports learning and reporting, and allows NHRIs to scale their activities without proportionally increasing costs.

At the same time, digitization carries risks. NHRIs handle sensitive information, and poor systems can expose individuals to privacy breaches, security threats, or exclusion of those without digital access. There are also risks to institutional independence and long-term sustainability if systems are poorly governed or overly dependent on external vendors.

Digitization is acceptable when benefits clearly outweigh harm and there are clearly mandated objectives. Below we unpack ten critical risks and the necessary mitigating actions to ensure benefits outweigh harm.

Table 1 **Risks and barriers of digitization**

CATEGORY	RISK	MITIGATING ACTION
Rights & Legal Risks	<p>Privacy & data protection</p> <p>Complaints systems may process sensitive data from survivors of sexual and gender-based violence, Human Rights Defenders (HRDs), minors, etc. Unclear legal bases, weak consent flows, or over collection can violate domestic data-protection laws and international standards. High-risk processing (monitoring, large-scale sensitive data) typically requires a Data Protection Impact Assessment (DPIA) before services go-live.</p>	<p>Mandate DPIA</p> <p>Make DPIAs compulsory for all new systems before they go live. This ensures the system is designed to practice data minimization—collecting only the information that is strictly necessary.</p> <p>Ensure transparency: Publish privacy notices in plain, local languages on all public-facing interfaces (websites, kiosks, etc.) so the public clearly understands how their data is used.</p>
	<p>Surveillance & network interference</p> <p>Network shutdowns, throttling, and targeted surveillance can block access and availability to NHRI platforms. Potentially endangering complainants and witnesses.</p>	As above.

3 Office of the United Nations High Commissioner for Human Rights, Human Rights Due Diligence for Digital Technology Use: Guidance of the Secretary-General, United Nations, 2023 (<https://www.ohchr.org/en/documents/tools-and-resources/human-rights-due-diligence-digital-technology-use-guidance-secretary>)

Safety & Do-No-Harm Risks

Data Security
& Cyber Security

Retaliation risks

Leaked identities or data could lead to retaliation, particularly against complainants and HRDs.

- ↳ **Implement Roles Based System Access Control (RBAC):** Configure systems so that staff can only access the specific data required for their job function. This will minimize access to sensitive data by unauthorized personal.
- ↳ **Data security:** Protect data through encryption at rest (in the database), encryption in transit (over the network), and multi-factor authentication for system access. Ensure alignment with recognized cybersecurity standards (such as NIST and ISO/IEC 27001), conduct regular cyber-awareness drills for staff, and perform routine cyber-hygiene checks across systems and user devices.
- ↳ **Cybersecurity governance and risk management:** Establish a formal security governance framework before launching and operating digital services, including clearly defined security roles and risk owners, documented security policies and procedures, third-party and supplier security risk management, and mechanisms for continuous security improvement.

Inclusion, Accessibility & Language Risks

Digital exclusion

The “digital divide” (cost of data, devices), disability barriers, and language gaps can systematically exclude rural or vulnerable communities from accessing digital channels.

- ↳ **Offer multi-channel intake:** provide diverse reporting options including Web, WhatsApp, SMS, and USSD (remembering however that channels such as SMS and USSD are not secure – can be used for non-sensitive comms) to reach users across different technological levels.
- ↳ **Ensure accessibility compliance:** strictly follow Web Content Accessibility Guidelines (WCAG 2.1 AA) and support local languages.
- ↳ **Reduce financial barriers:** make sure reporting by SMS or USSD is free for users, so complainants do not have to pay to submit a report.
- ↳ Provide **alternative reporting channels**, including voice-based or assisted complaint submission.
- ↳ Allow **trusted intermediaries** such as civil society organizations or community leaders to support individuals in lodging complaints through a secure NHRI web portal.

Inclusion, Accessibility & Language Risks

In addition to language and disability considerations, NHRIs should also take into account broader accessibility challenges. In many contexts, potential complainants may have low levels of literacy, limited internet connectivity, or may rely primarily on oral communication channels. Survivors of human rights violations may also require trauma-sensitive reporting pathways. Without appropriate design considerations, digital systems may unintentionally exclude vulnerable populations or discourage reporting.

- ↳ Ensure systems can function in **low-bandwidth or intermittent connectivity environments**.
- ↳ Consider **trauma-sensitive reporting processes** for vulnerable or at-risk complainants.

Data Quality, Integrity & Chain-of-Custody Risks

Evidence integrity

Unstructured uploads, weak metadata, and poor audit trails undermine the credibility of investigations as well as public trust.

- ↳ **Enforce structured data:** use standardized forms that automatically capture evidence metadata (e.g., timestamps, GPS coordinates etc.).
- ↳ **Guarantee auditability:** implement immutable audit logs (tamper-evident records that cannot be altered) to track every action taken on a file.
- ↳ **Secure chain-of-custody:** design the system to separate allegation, evidence, and analysis datasets. Enable strict version control to track any edits made during the investigation process.

Interoperability, Vendor Lock-In & Sovereignty Risks

Vendor lock-in

Closed, proprietary systems can block integration with partners (e.g., police referrals) and make it difficult to migrate data if the NHRI wants to change systems later.

- ↳ **Prioritize open standards:** procure or develop systems based on open standards to ensure they are not restrictive.
- ↳ **Secure data ownership:** ensure Service Level Agreements (SLAs) contain explicit exit clauses (data export and transitional support), and state that the NHRI owns all data, system product licenses, and key system/service components.
- ↳ **Plan for the exit:** include clear exit clauses in contracts that guarantee data portability and transitional support to prevent being locked into a single vendor.

Interoperability, Vendor Lock-In & Sovereignty Risks

Data Sovereignty

Third party systems may not adhere or be subject to countries data laws.

- ↳ **Ensure sovereignty:** SLA's must align all data usage regardless of their location in accordance with the country's laws and regulations. Ensuring data sovereignty and ownership.

Data residency and jurisdictional risk

When systems are hosted in foreign jurisdictions, national laws in those countries may allow authorities to compel access to stored data. For NHRIs handling politically or otherwise sensitive complaints, documentation of human rights violations, this raises concerns regarding confidentiality, institutional independence, and protection of complainants. Institutions should carefully assess where their data is stored, which jurisdiction governs the hosting provider, and what legal mechanisms may allow third-party access.

- ↳ Assess data residency requirements before procurement.
- ↳ Ensure contracts clearly define data ownership and jurisdiction.
- ↳ Prefer hosting environments that ensure NHRI control over sensitive data.

Governance, Independence & Political Pressure Risks

Political interference

Digitized case data can be targeted for political interference or mass disclosure requests.

- ↳ **Codify independence:** embed safeguards directly into the governance structure. This includes strict system/service access approvals and digital Standard Operating Procedures (SOPs).
- ↳ **Protect sensitive reporting:** implement transparent reporting protocols that protect sensitive individual data, ensuring transparency does not compromise safety.
- ↳ **Define escalation paths:** establish clear routes to NHRI leadership for handling external pressure or disclosure requests. (As per established NHRI practice).

Sustainability & Capacity Risks

Under-resourcing

Lack of budget for maintenance or training leads to fragile systems. Donor-driven platforms may not align with the NHRI's actual mandate.

- ↳ **Budget for total cost of ownership:** plan finances beyond the initial build to include licenses, hosting, SMS, support, and security testing.
- ↳ **Build internal capacity:** invest in continuous training for both investigators and IT staff.
- ↳ **Plan for continuity:** schedule a 5-year technology refresh. Maintain paper/offline fallbacks and tested Disaster Recovery (DR) plans to ensure operations continue if digital systems fail.

AI/Automation Risks

Bias & Due Process

AI models used to triage complaints, reporting, human rights documentation, may introduce hidden biases. Furthermore, automated decisions often lack explainability, which may undermine a complainant's right to appeal if they cannot understand the logic behind a decision.

- ↳ **Keep humans in the loop:** ensure all automated decisions are logged and subject to human review/interrogation. Publish model use notices.

Data Leakage & Interference

There is a specific risk of inadvertent disclosure of sensitive data via model telemetry (coded or AI-generated technical data sent back to providers). Additionally, connecting to third-party Application Programming Interface (APIs) may introduce vulnerabilities or allow external actors to interfere with the system.

- ↳ **Preserve privacy:** use privacy-preserving configurations to prevent data leakage via model telemetry.
- ↳ **Restrict external data sharing:** prohibit sending sensitive content to external AI models unless a strict Data Processing Agreement (DPA) is in place.

AI Misuse or Manipulation

AI tools may be intentionally misused to generate misleading analysis, manipulate case prioritization, or produce fabricated reports. In sensitive human rights contexts, malicious actors could attempt to influence data inputs or exploit system vulnerabilities in order to distort investigative outcomes or undermine institutional credibility.

- ↳ Establish clear institutional policies defining acceptable AI use within NHRI systems.
- ↳ Implement strict access controls and authentication for AI-enabled features.
- ↳ Maintain system audit trails to detect unusual activity or data manipulation.
- ↳ Require validation and verification of data sources used in AI-supported analysis.

AI/Automation Risks**AI ‘Hallucinations’ and Incorrect Outputs**

AI systems may generate outputs that appear plausible but are factually incorrect or unsupported by evidence. In investigative or reporting contexts, this could lead to inaccurate analysis, misinterpretation of complaints, or incorrect recommendations if AI outputs are accepted without verification.

- ↳ Require human validation of all AI-generated summaries, recommendations, or analyses.
- ↳ Use AI primarily as a decision-support tool rather than a decision-making authority.
- ↳ Train staff to understand AI limitations and recognize potential inaccuracies.
- ↳ Clearly label AI-generated outputs within the system to ensure transparency.

Evidence of Impact vs. Activity**Metric relevance**

Dashboards often track “vanity metrics” (simple activity counts) rather than actual human rights outcomes (resolution, safety).

- ↳ Define meaningful indicators: shift focus to Monitoring, Evaluation, and Learning (MEL) metrics that matter. Measure real-world impact, such as time-to-assignment, 30/60/90-day closure rates, survivor safety checks, and accessibility metrics.

3. CASE EXAMPLES: NHRI DIGITAL STRATEGY AND SYSTEMS COMPARISONS

NHRIs increasingly rely on digital tools to strengthen their ability to receive complaints, manage cases, document human rights violations, public outreach and respond to human rights violations in a timely and transparent manner. The starting points for digital transformation often differ across institutions. The following case examples illustrate how two NHRIs – the National Commission for Human Rights of Pakistan and the National Human Rights Commission of Nigeria have progressively introduced digital systems to strengthen complaint handling, improve institutional coordination and expand public access to reporting channels. While each institution followed its own path shaped by national context, resources, and institutional priorities, both demonstrate how targeted digital investments, phased implementation can significantly improve operational effectiveness and service delivery. These examples highlight practical lessons for NHRIs seeking to improve digital readiness while maintaining a focus on accessibility, transparency, and institutional sustainability.



CASE EXAMPLE

THE NATIONAL COMMISSION FOR HUMAN RIGHTS (NCHR) OF PAKISTAN



Institutional context

The NCHR of Pakistan was established in accordance with the National Commission for Human Rights Act of 2012, with a mandate to promote and protect human rights in accordance with the country's constitution and international human rights obligations.

Following the appointment of its Chairperson and members in November 2021, the NCHR resumed operations with a modest institutional footprint and low digital maturity. Internal coordination relied heavily on manual processes, office ICT capacity and infrastructure was limited, and case tracking and reporting systems were fragmented across headquarters and provincial offices.

To address these constraints, from 2023, the NCHR's leadership prioritized institutional strengthening, focusing on improving governance, formalizing internal procedures, and enabling provincial offices to operate more autonomously within defined SOPs. This decentralized approach sought to improve responsiveness to the public while maintaining institutional coherence between headquarters and provincial offices.

As an initial "quick win" the NCHR's leadership turned to ICT as a means to fill gaps identified. The NCHR introduced a formalized organizational email capability to support secure official communication across offices, supported through a third-party service arrangement, alongside practical ICT remediation measures such as refurbishing and upgrading legacy computing equipment to extend usability and improve baseline productivity.

Today, the NCHR is actively making use of technology to be more proactive than reactive. Chatbots, a triage system and automation are working to enhance the service offerings to the Pakistani public.



Solution overview

In 2022, the NCHR developed a Strategic Plan with numerous national consultations, that identified digital transformation as an institutional priority. A detailed technology assessment with both headquarters and provincial offices was subsequently undertaken to identify short-, medium-, and long-term ICT needs and priorities.

Following completion of this assessment, the NCHR launched a technology initiative focused on establishing and strengthening its public-facing digital presence. This included developing an updated web presence, activation of official social media channels, and the design of a structured digital communications approach to improve outreach and public awareness.

A key priority was addressing a backlog of more than 10,000 complaints across headquarters and provincial offices. The NCHR supported through SLA initiated the development of a digital complaints management system to enable provincial offices to register and manage complaints end-to-end, while also supporting consolidated reporting at the institutional level. This represented a shift away from mainly manual processes and enabled more consistent tracking, visibility, and reporting across the NCHR.

As part of establishing the NCHR's operating structure, the leadership implemented standardized filing, monitoring and investigation systems across its offices. To support consistent reporting against agreed data sets, the Commission engaged external consultants to replace the ad hoc WhatsApp-based approach that had been used previously. A standard reporting template was introduced, alongside a more structured and reliable communications process.



Technical implementation

In 2023, the NCHR reached an important turning point. It began receiving consistent operational funding from government, which assisted in establishing a foundational ICT environment in which further systems could be designed, built and deployed. These developments marked the beginning of a gradual increase in digital maturity, where the benefits of earlier technology investments were becoming evident. During this period, the NHRC also began exploring open-source technologies as a practical and cost-effective means of addressing ongoing resource constraints.

Between 2023 and 2024, the NCHR initiated efforts to align its internal technology environment with Pakistan's broader national digital approach. This alignment was viewed as a strategic opportunity to develop a structured digital transformation roadmap that would improve service delivery while remaining consistent with government-wide ICT standards and practices. As part of this process, the NCHR developed an important 'Safety & Security' policy for the Governments Digital Inclusion Strategy and recruited its first full-time ICT officer, whose responsibilities included managing existing technology platforms, providing user training and support, and coordinating with external technology vendors.

Over the following months, the NCHR expanded its internal ICT capacity by recruiting additional technical staff and undertaking a comprehensive technology reassessment. This assessment evaluated both the NCHR's immediate operational requirements and its longer-term digital needs. Key focus areas included hardware infrastructure, software platforms, data management, and systems integration. A central principle that emerged from the review was the need for proper role separation within the ICT environment.

During this same period, several practical digital initiatives were already underway. The NCHR used algorithms to track hate speech following [the violence in Jaranwala⁴](#) and introduced basic project management tools, internal databases, and an initial dashboard capability to support monitoring and reporting. Rather than relying on a single system, NCHR adopted a hybrid technology approach, combining locally hosted tools with externally supported platforms to meet its varied operational requirements in a flexible and affordable manner.

A major milestone was the introduction of the Online Complaint Management Portal. Rather than replacing the existing manual processes for lodging complaints, the portal complemented them by providing the Commission with an additional formal digital intake channel. The portal enabled individuals and groups to submit human rights complaints electronically, upload supporting documentation, and track case status remotely. This marked a significant shift away from purely paper-based processes and allowed the NCHR to expand access to its services beyond physical office locations.

The online portal also strengthened internal case management by creating a centralized repository for complaints and related records. It improved data consistency, supported more efficient workflow tracking, and enhanced transparency in how cases were received and processed. Although still evolving, the portal represented a critical step toward a more structured, technology-enabled complaints handling system and laid the groundwork for future integration with other digital tools and reporting mechanisms.



Impact

- ↳ **Continuity:** the launch of the [Online Complaint Management System](#) has enabled individuals to submit, upload documents, and track human rights complaints digitally thereby increasing the outreach of the NCHR and ensuring compliance with the Paris Principles. This has ensured that the NCHR can continuously receive and process cases without relying solely on paper-based or in-person channels. This digital intake layer supports uninterrupted case handling across the entire country.
- ↳ **Reach & access:** the NCHR's digital complaint portal has provided a nationwide public intake channel that lowers reporting barriers, offering remote access regardless of a citizen's location, complementing the NCHR's regional offices.
- ↳ **Scale of complaints captured:** the current NCHR's annual reporting system enables online submissions and real-time tracking of complaints.
- ↳ **Visibility & policy response:** by facilitating digital tracking and transparency, the online portal supports the NCHR's ability to monitor human rights trends and produce more consistent reporting.
- ↳ **Case integrity:** the digital infrastructure of the complaint management system increases data integrity and traceability as well as providing a mechanism to upload any supporting documents that may be of use. Additionally, the system electronic tracks cases and enables more consistent case recording.

4 National Commission for Human Rights Pakistan, 'Jaranwala Incident Report', National Commission for Human Rights, Islamabad, 2023



Implementation insights

The NCHR underscored the importance of digitally minded leadership. Its leadership demonstrated the foresight to leverage technology to strengthen both internal operations and external service delivery. Importantly, embedding technology priorities within the Strategic Plan helped formalize the role of technology and provided a clear institutional mandate for digital transformation. Rather than moving prematurely, the NCHR took a measured approach, testing and validating priorities before scaling implementation, which has yielded positive results. The NCHR has also aligned its initiatives with Pakistan's national digital approach and is benefiting from that alignment.



Sustainability and scaling

With an overall vision that places people first and prioritizes public access, the planned introduction of a customer relationship management (CRM) system, enhancements to the data dashboard, and the future implementation of chatbots and a triage capability are intended to strengthen population-facing services. These initiatives will be complemented by a stronger focus on inter-agency integration. These initiatives aim to position the NCHR as a more proactive institution capable of responding rapidly to emerging human rights issues.



Challenges & lessons learned

In its early years, the NCHR faced significant constraints in developing its digital capabilities including limited ICT capacity, with few staff possessing the technical skills required to support a comprehensive digital strategy, outdated systems – not well suited to its operational needs and did not effectively support its core functions.

Adoption of new technologies was initially slow, as some operational staff were hesitant to transition to digital systems. Connectivity between the central office and regional offices was also unreliable, which limited information sharing and system integration. Furthermore, many basic ICT services and infrastructure were not yet in place, requiring the Commission to first establish foundational digital capabilities.

The NCHR's experience demonstrates the value of a phased and strategic approach to digital transformation. Rather than implementing large-scale systems immediately, the NCHR introduced basic digital components first and gradually expanded its capabilities over time. Continuous internal engagement and awareness-building helped increase staff confidence in using new systems. In addition, partnerships with private sector technology providers helped address technical and capacity gaps, enabling the NCHR to progressively strengthen its digital infrastructure and services.



CASE EXAMPLE

THE NATIONAL HUMAN RIGHTS COMMISSION (NHRC) OF NIGERIA



Institutional context

In 2020, the NHRC of Nigeria digitized its manual complaints registration and case-tracking processes to maintain operational continuity during the COVID-19 lockdowns. During this period, the move proved critical as [reports](#) of human-rights violations increased.⁵

Prior to digitization, complaints were primarily registered manually and tracked through paper records, making it difficult to manage cases across the NHRC's nationwide network of offices. The pandemic accelerated the need for remote reporting channels and reliable digital case management.



Solution overview

The initial application developed, supported all 36 states but was centrally managed, meaning HQ assigned cases to state offices, and state investigators allocating work internally. The status and evidence of each case was in turn returned to HQ electronically for statistical reporting purposes. Today, NHRC's public channels include an [online complaint form](#)⁶ and the Human

5 National Human Rights Commission Nigeria, 'Report of Alleged Human Rights Violations Recorded Between 13th April to 4th May 2020 Following the Extension of the Lockdown Period', National Human Rights Commission, Abuja, 2020.

6 National Human Rights Commission Nigeria, 'Complaint Form', National Human Rights Commission, Abuja, n.d.

Rights Abuse Tracking (HRAT) portal, reflecting this digital shift and an alignment to Nigeria's Digital Transformation strategy.

The initial system was a web-based complaints registration tool that ensured that individuals could continue submitting complaints while physical offices were closed. It then matured into an electronic complaint-tracking system with user accounts, role-based access, and case assignment from HQ to state offices.

NHRC's public intake now spans the online complaint form, the Human Rights Abuse Tracking reporting portal, and a mobile app, broadening access for complainants beyond walk-ins and letters. Integration with the Commission's toll-free short code (6472)/call center supports hybrid intake.⁷

Additionally, the development of a mobile solution (platform agnostic) integrating with the call-center channel will further enhance accessibility and usability, especially for communities with intermittent broadband but reliable mobile coverage. (NHRC's HRAT app is already listed on Google Play.)⁸



Technical implementation

Following internal reviews, the NHRC decided to work with an external technology vendor to develop implementation and operate the system, while retaining institutional ownership of policies, processes, data and the system as a whole.

The current system is a centralized proprietary web-based application with:

- a) structured digital forms mapped to NHRC case categories,
- b) HQ case triage & assignment to state offices,
- c) investigators work queues,
- d) digital evidence and document uploads,
- e) audit trails, and
- f) management dashboards for HQ and state leadership.

Data handling aligns to Nigeria's Data Protection Regulator (NDPR - purpose limitation, lawful basis, consent/notice, security, and audit filing),⁹ and the NDPR Implementation Framework (2020) provides the compliance requirements for audits and vendor oversight.



Impact

- ↳ **Operational continuity:** the digital reporting channels allowed the NHRC to continue receiving and processing complaints when physical offices were constrained or closed during COVID-19 lockdowns.
- ↳ **Expanded reach & access:** public intake channels (web form; HRAT portal; call center 6472) lowered barriers to reporting across Nigeria's states, complementing NHRC's nationwide office footprint.
- ↳ **Scale of complaints captured:** NHRC reports over 2,000,000 complaints in 2024,¹⁰ monthly dashboards in 2024–2025 show sustained high volumes, validating the need for a robust digital pipeline.

7 National Human Rights Commission Nigeria, 'Official Website', National Human Rights Commission, Abuja, n.d.

8 Google, 'HRAT Mobile Application', Google Play Store, Google LLC, Mountain View, n.d.

9 National Information Technology Development Agency, 'Nigeria Data Protection Regulation', National Information Technology Development Agency, Abuja, 2019.

10 National Human Rights Commission Nigeria, 'Human Rights Assessment Dashboard for the Year 2024', National Human Rights Commission, Abuja, 2024.

- ↳ **Visibility & policy response:** the web-based Human Rights Situation Dashboards (Dec-2024, monthly in 2025) providing trends on cases such as SGBV and child-rights violations.¹¹
- ↳ **Case integrity:** centralized tracking and audit trails support complex investigations that require transparent chains of custody for evidence and findings as illustrated by NHRC's special-panel process (2023–2024).¹²



Implementation insights

The NHRC stressed the value of starting with a simple digital tool –launching with basic, reliable complaints registration, then iterating into full tracking. This **phased approach** avoided over-stretching technical and financial resources. Aligning with the Nigeria Data Protection Regulation (NDPR) and its 2020 Implementation Framework helped embed security, lawfulness, and auditability from the outset, which improved public confidence in digital reporting.



Sustainability and scaling

The current system is hosted in a cloud environment, which supports high availability and built-in redundancy. High availability means the system is designed to remain operational and accessible with minimal interruption. While built-in redundancy means that key system components are duplicated, so that if one component fails, another can take over and keep the system running. The NHRC maintains a detailed SLA with the vendor for uptime and support. Source code and technical documentation are available to NHRC's internal technical team, enabling a credible pathway to greater internal ownership if required. At present the NHRC has an internal technical team which is working alongside their vendor counterparts as part of a knowledge sharing agreement.

The current roadmap includes interoperability, linking with the Nigeria Police and protection-mandated institutions, so referrals and follow-ups can move faster while preserving privacy under NDPR controls (data-sharing memorandum of understanding, role-based access, and audit logs).



Challenges and lessons learned

Prior to digitization, the NHRC relied heavily on manual complaint registration and paper-based case tracking, which made it difficult to manage cases across its nationwide offices. Ensuring accessible reporting channels for the public, particularly in areas with limited internet connectivity, and maintaining compliance with NDPR were of paramount importance. Beginning with a simple web-based complaints registration tool to ensure operational continuity during the pandemic. The system was later expanded into a full electronic case-tracking platform with role-based access control, digital evidence management, and centralized reporting.

Collaboration with a technology vendor also helped address technical capacity gaps while ensuring the NHRC retained ownership of its processes, data, and governance frameworks.

“Digital maturity” describes how an institution’s digital systems and capacities are. This includes connectivity, cybersecurity, equipment, and basic digital skills among staff. NHRIs are encouraged to assess their digital maturity as a basis to better plan to further advance their digital readiness. “Digital maturity” describes how an institution’s digital systems and capacities are. This includes connectivity, cybersecurity, equipment, and basic digital skills among staff. NHRIs are encouraged to assess their digital maturity as a basis to better plan to further advance their digital readiness.

11 National Human Rights Commission Nigeria, ‘December 2024 Human Rights Dashboard’, National Human Rights Commission, Abuja, 2024.

12 Reuters, ‘Nigerian Rights Body Ends Probe into Abortion Allegations Against Military’, Reuters, London, 2024.

Part 2

**DIGITAL MATURITY &
DIGITAL READINESS
CHECKLISTS**



1. DIGITAL MATURITY ASSESSMENT

The **five-level maturity scale** (**RED** = low, **YELLOW** = medium and **GREEN** = high maturity):

**Level
1**

Manual/Analog
Fully paper-based

**Level
2**

Emerging
Some digital processes, mostly still pap -driven with no integration

**Level
3**

Developing
Integrated systems, limited automation

**Level
4**

Advanced
End-to-end digital workflows, real-time data use

**Level
5**

Mature
Has a strong and stable digital foundation and is able to plan for continuous improvement. The institution can assess and, where appropriate, adopt new technologies, including artificial intelligence, to strengthen systems, processes, and service delivery in a responsible and well-governed manner.

1.1 DIGITAL MATURITY LEVEL INDEX

The table below highlights the digital maturity levels, their institutional characteristics, digital systems operations and whether AI is in operational use.

Table 2

MATURITY LEVEL	INSTITUTIONAL CHARACTERISTICS	DIGITAL SYSTEMS AND OPERATIONS	AI READINESS / USE
Level 1 Manual / Analog	The institution operates largely through paper-based systems and manual processes. Staff exposure to digital tools is limited, and digital awareness is generally low. Leadership may recognise the potential value of technology, but digital planning is minimal or absent.	Case intake, case tracking, reporting, records management, and communications are largely manual. Technology use is limited to basic office tools, if available, and there is little or no structured ICT support.	AI is not in operational use. The institution has limited capacity to assess, procure, govern, or monitor AI-enabled tools. Immediate priorities are likely to be basic digital awareness, foundational governance, and minimum safeguards.
Level 2 Emerging	The institution is beginning to adopt digital tools in selected areas, but use remains fragmented and often depends on individual initiative. Digital awareness is growing, but institutional capacity and governance remain limited.	Some processes are digitised, such as email, spreadsheets, word processing, or digital document storage. Paper-based and digital processes coexist, but there is little integration and limited standardization.	AI may be discussed or informally explored, but there is no structured institutional approach to assessing suitability, risks, oversight, or safeguards.
Level 3 Developing	The institution has established a clearer direction for digital development and is strengthening internal capacity, governance, and operational support. Staff are becoming more confident in the use of digital tools, although maturity may vary across teams.	Partial case management tools, online forms, digital records, shared drives, dashboards, or reporting systems may be in use. Infrastructure is improving, and some processes are supported by both local and online systems. Governance, training, and support arrangements are developing but may still be uneven.	The institution may be exploring limited AI use for narrow administrative or analytical purposes, such as translation, triage support, knowledge retrieval, or drafting assistance. Any such use should remain cautious and subject to human oversight, basic risk assessment, and data protection safeguards.

Level 4 Advanced

The institution demonstrates strong digital capability across multiple functions. Digital systems are increasingly embedded into operations and service delivery, and governance arrangements are more established and better understood.

End-to-end or near end-to-end workflows are supported through integrated digital systems. Staff collaborate through shared platforms, cloud tools, and data dashboards. Cybersecurity, backups, user access controls, and compliance mechanisms are applied more consistently.

AI-enabled tools, where used, are introduced selectively for clearly defined purposes and are supported by governance measures such as policy controls, human review, role clarity, accuracy checks, privacy safeguards, and oversight of bias and accountability risks.

Level 5 Mature

The institution has a well-established and sustainable digital operating environment. Leadership, operational teams, and technical support functions work together strategically to review, strengthen, and continuously improve digital systems and governance over time. Digital planning is embedded in institutional decision-making and aligned with the NHRI's mandate, priorities, and long-term development.

Digital systems are stable, integrated, and consistently used across relevant functions. Processes are well governed, monitored, and regularly improved. The institution is able to manage digital risks, maintain continuity, use data more effectively for planning and reporting, and adapt systems in response to changing operational, legal, or contextual needs.

The institution is able to assess, govern, and, where appropriate, responsibly use AI-enabled tools within a clear ethical, legal, and operational framework. AI use is not assumed or required, but where adopted it is subject to robust human oversight, transparency, risk mitigation, and rights-based safeguards.

1.2 MATURITY AND CAPABILITY PROGRESSION FRAMEWORK

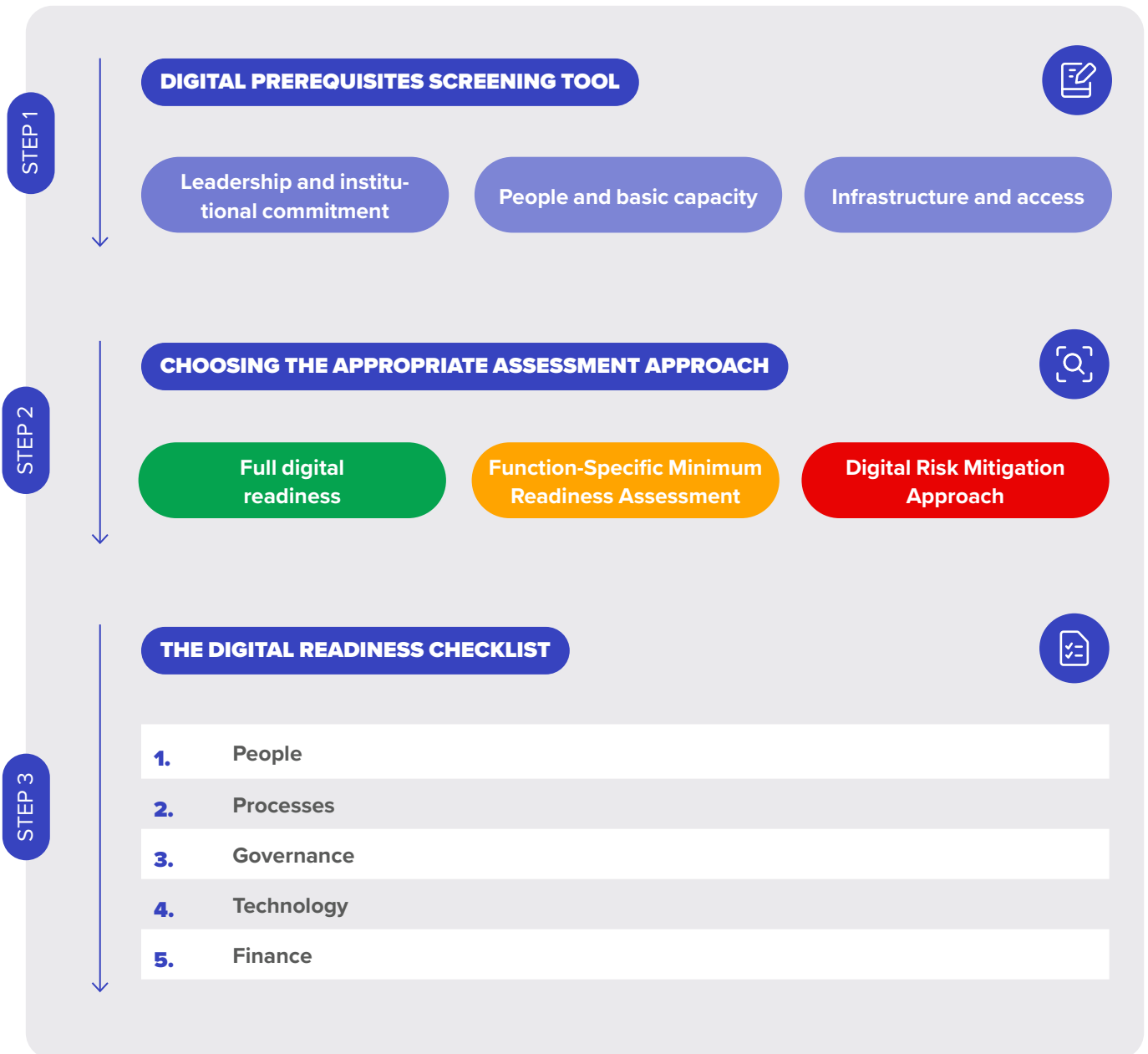
Table 3

The table below is intended to help NHRIs identify their current level of digital maturity across key institutional dimensions, so that they can better understand existing strengths and gaps, set realistic priorities, and plan practical, proportionate steps for digital improvement.

DIMENSION	LEVEL 1 MANUAL / ANALOG	LEVEL 2 EMERGING	LEVEL 3 DEVELOPING	LEVEL 4 ADVANCED	LEVEL 5 MATURE
People & Leadership	Leadership engagement is limited, and staff confidence in digital tools is generally low. Digital change may be seen as difficult, risky, or unnecessary.	Leadership has identified digital priorities, and staff are increasingly able to support day-to-day digital activities. Responsibility for digital matters is becoming clearer.		Leadership, operational teams, and technical personnel work together strategically. Digital thinking is embedded across the institution, and continuous improvement is encouraged.	
Technology & Infrastructure	Technology use is minimal and may be limited to basic office tools. Infrastructure, connectivity, devices, and technical support are weak or inconsistent.	Basic digital tools are being introduced in selected areas. Devices, connectivity, and support arrangements are improving, but remain limited and fragmented.	Core infrastructure is in place to support routine digital operations. Systems, devices, connectivity, and support arrangements are becoming more reliable.	Digital systems are established across multiple functions, supported by stronger infrastructure, user management, backup processes, and technical support.	Technology and infrastructure are stable, well governed, and able to support optimization, resilience, and future innovation.
Processes and Service Delivery	Most operational processes are manual or paper based, with only limited digital assistance.	Selected processes are supported by basic digital tools, but paper-based and digital processes still coexist with little integration.	A growing number of operational processes are supported by digital systems, including selected workflows, records, forms, or reporting tools.	Most processes that are appropriate for digitization are supported by digital systems, with stronger integration across workflows and service delivery.	Digital processes are embedded across the institution, and new operational needs are routinely assessed for proportionate digital solutions.

Governance, Frameworks, and Good Practice	Formal digital governance, standards, policies, and best-practice frameworks are largely absent or not applied consistently.	Basic policies, controls, or reference frameworks may exist, but alignment is limited and implementation remains uneven.	Governance arrangements, policies, and selected good-practice frameworks are being adopted to guide digital planning, security, and service management.	Governance arrangements are established and applied consistently. Recognized frameworks and good practices are informing security, continuity, accountability, and improvement.	Digital governance is mature and forward-looking. The institution reviews and refines its controls, frameworks, and practices in response to evolving needs and risks.
Training and Capacity Development	Structured digital training is limited or absent, and staff mainly rely on informal self-learning.	Basic training is beginning to take place, usually for selected users or in response to immediate operational needs.	Training is available and increasingly aligned with the systems and processes being introduced. Capacity development is becoming more structured.	Training is routinely available, encouraged, and linked to operational roles, digital responsibilities, and system changes.	Continuous learning is embedded in the institution. Training is available across levels and supports both current capability and future digital development.
AI Readiness and Governance	AI is not in operational use, and the institution has limited capacity to assess, procure, govern, or monitor AI-enabled tools.	AI may be discussed or informally explored, but there is no structured institutional approach to assessing relevance, risks, or safeguards.	Limited AI-enabled tools may be explored for narrow support functions. Any use is cautious and should remain subject to human oversight and basic safeguards.	Where used, AI-enabled tools are introduced selectively for defined purposes and are supported by governance measures such as policy controls, review mechanisms, and privacy safeguards.	The institution is able to assess and, where appropriate, responsibly govern AI-enabled tools within a clear ethical, legal, and operational framework.
Key Challenges and Risks	Common constraints include limited funding, weak infrastructure, low digital skills, and limited institutional confidence in digital change.	Challenges often include fragmented systems, inconsistent skills, limited budgets, and uncertainty about how to scale digital improvement safely.	Common pressures include uneven implementation, dependence on a small number of staff or suppliers, resource constraints, and the need to strengthen governance and sustainability.	Challenges may include maintaining quality, funding ongoing upgrades, managing change, and ensuring that governance, security, and compliance keep pace with expansion.	Key risks include complacency, over-complexity, unsustainable innovation, or adopting new technologies faster than the institution can govern, maintain, or justify them.

2. INTRODUCTION TO THE DIGITAL READINESS CHECKLIST



The Digital Readiness Checklist should be used as a practical self-assessment tool to guide reflection, planning, and prioritization across the core dimensions of people, processes, governance, technology and finance. The completion of the Checklist is best done collaboratively, with input from leadership, operational staff, ICT support personnel, legal or compliance teams, and other relevant stakeholders where available.

Before completing the full checklist, institutions are encouraged to first complete the **Digital Prerequisites Screening Tool**. This helps determine whether minimum enabling conditions are in place for a meaningful readiness assessment and supports the selection of the most appropriate assessment pathway. In this way, the checklist is intended to remain flexible, modular, and actionable across a wide range of NHRI contexts.

The purpose of this checklist is not to evaluate institutions against a single standard of “digital maturity,” nor to assume that all NHRIs should pursue full digital transformation at the same pace or in the same way. Rather, it is intended to help institutions identify their current position, understand foundational gaps, recognize areas of strength, and determine practical next steps. In some cases, this may mean preparing for broader digital transformation. In others, it may mean focusing first on basic enabling conditions, targeted functional improvements, or digital risk mitigation for systems already in use.

2.1 STEP 1: DIGITAL PREREQUISITES SCREENING TOOL



The short screening tool is intended for institutions at an early stage of digital development, particularly those operating in low-sourced or digitally constrained contexts. Its purpose is not to assess full readiness, but to identify whether the institution is ready to proceed with a **broader assessment** or whether it should first focus on **foundational actions**.

This screening should be completed using simple responses of *Yes, Partly, or No*.

- ↳ A result of “Mostly Yes” suggests that the institution can proceed to the full checklist.
- ↳ A result of “**Mostly Partly**” suggests that the institution can proceed but should **prioritize foundational improvements** alongside the assessment.
- ↳ The result of “**Mostly No**” suggests that the institution should first **focus on basic leadership, capacity, infrastructure, governance, and protection measures** before undertaking a fuller digital readiness assessment.

The absence of prerequisites should not be seen as failure. Rather, it should help the NHRI identify immediate enabling actions that make future digital transformation realistic, safer, and more sustainable.

Table 4 **Digital pre-requisites**

DOMAIN	PREREQUISITE SCREENING QUESTION	RESPONSE (YES / PARTLY / NO)	IMMEDIATE ACTION IF GAP EXISTS
Leadership and institutional commitment	Is leadership supportive of digital improvement or digital reform?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Build leadership awareness and agree on a practical digital priority.
	Has the NHRI assigned at least one person to coordinate digital matters, ICT support, or innovation?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Assign a focal point or secure external support to coordinate digital issues.
	Are there clear institutional priorities for why digital tools are needed, even if only for one or two functions?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Clarify the initial use case, such as complaints intake, case tracking, or reporting, documentation, follow up.

People and basic capacity	Do staff have access to basic digital tools such as email, office applications, and secure communications?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Provide access to minimum productivity and communication tools.
	Do enough staff have basic digital skills to use routine digital tools safely and consistently?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Provide basic digital literacy and cyber hygiene support.
	Is there at least some internal or external ICT support available to maintain basic systems and respond to problems?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Identify an ICT resource, service provider, or partner for ongoing support.
Infrastructure and access	Do the NHRI's main service locations have reliable electricity?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Address power resilience, backup power, or phased service-point rollout.
	Do the main service locations have internet access that is usable for routine operations?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Prioritize connectivity solutions or limit digital rollout to connected locations first.
	Are enough devices available for staff to carry out digital tasks without severe sharing constraints?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Prioritize minimum device access for key staff and service points.
Minimum protection and continuity	Are basic cybersecurity measures in place, such as antivirus, firewalls, password controls, and secure access practices?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Implement basic security controls before expanding digital services.
	Are important files or records backed up in some regular and reliable way?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Establish a simple, routine backup and recovery process.
	Has the NHRI considered where its data is stored and who is responsible for protecting it?	<input type="radio"/> Yes <input type="radio"/> Partly <input type="radio"/> No	Clarify data storage, ownership, and responsibility arrangements.

2.2 STEP 2: CHOOSING THE APPROPRIATE ASSESSMENT APPROACH



Once the Digital Prerequisites Screening Tool has been completed, the NHRI should select the assessment approach that best reflects its current context, institutional priorities, available capacity, and level of digital ambition. The purpose of this step is to ensure that the institution follows an approach that is realistic, proportionate, and actionable.

Not all NHRIs are starting from the same position. Some may already have enough foundational conditions in place to consider broader digital strengthening across the institution. Others may wish to focus only on one or two priority functions, such as complaints intake, case tracking, recommendation tracking, reporting, documentation of violations or records management. Others may not yet be planning wider digitalization, but still need to strengthen the safety, governance, and continuity of the digital tools they already use.

The approach selected should therefore reflect both the results of the prerequisites screening and the institution's immediate objectives. Once an approach has been selected, the NHRI should complete the Digital Readiness Checklist in a way that corresponds to that approach.

APPROACH 1 FULL DIGITAL READINESS ASSESSMENT

HIGH MATURITY LEVEL

This approach is appropriate for NHRIs that have sufficient foundational conditions in place and wish to assess readiness across the institution as a whole. **It should be used where the NHRI is considering broader digital strengthening across the core dimensions of people, processes, governance, technology and finance.**

This approach is generally appropriate where:

- ↳ The prerequisites screening shows mostly “Yes” or “Partly”
- ↳ Leadership is supportive of digital improvement
- ↳ Some ICT capacity or support is available
- ↳ The institution is seeking broader institutional strengthening rather than isolated digital interventions

→ Institutions following this approach should complete the Digital Readiness Checklist across all dimensions: *people, processes, governance, technology and finance*. The objective is to identify strengths, weaknesses, gaps, and priorities across the institution and to support broader digital planning and reform.

This approach is appropriate for NHRIs that are not yet ready for institution-wide digital transformation but wish to assess readiness for one or two specific functions. These may include complaints intake, case tracking, recommendation tracking, records management, reporting, or communications. This approach supports a phased approach and allows institutions to begin with practical, targeted priorities.

This approach is generally appropriate where:

- ↳ The prerequisites screening shows mixed readiness
- ↳ The institution has limited resources and needs to prioritize
- ↳ The NHRI wants to strengthen or digitize one or two functions first
- ↳ A gradual or phased approach is more realistic than institution-wide reform

→ Institutions following this approach should use the checklist selectively, focusing only on the sections most relevant to the function or processes they wish to strengthen. The aim is to assess whether that function can be digitized or improved safely, effectively, and sustainably, without needing to complete the entire checklist at the outset.

This approach is appropriate for NHRIs that are not currently planning significant digitalization, but already use some digital tools such as email, spreadsheets, shared drives, messaging platforms, websites, or basic databases. In these cases, the immediate priority is not broad digital transformation, but **ensuring that existing digital practices are safer, more resilient, and better governed.**

This approach is generally appropriate where:

- ↳ The prerequisites screening shows significant foundational gaps
- ↳ The institution is not yet ready for broader digital reform
- ↳ The NHRI still handles information through digital tools
- ↳ The immediate priority is security, continuity, data protection, and risk reduction

→ Institutions following this pathway should use the main checklist with a primary focus on those areas related to **digital safety, governance, continuity, and risk reduction.** In practice, this means paying particular attention to questions relating to governance arrangements, data protection, cybersecurity, access control, backup, storage, continuity, and the safe use of existing digital tools.

IMPORTANT NOTE

The approach selected does not prevent the NHRI from later moving to a broader assessment. An institution may begin with a function-specific or risk mitigation approach and, over time, progress to a fuller institutional digital readiness assessment as its capacity, confidence, and enabling conditions improve.

TIP: SIMPLE DECISION GUIDE

- ↳ **Mostly ready, and seeking broader institutional reform:**
follow the [Full Digital Readiness Assessment](#)
- ↳ **Partly ready, and focusing on one or two functions first:**
follow the [Function-Specific Minimum Readiness Assessment](#)
- ↳ **Not yet ready for wider digitalization but already using some digital tools:**
follow the [Digital Risk Mitigation Approach](#).

3. STEP 3: NHRI DIGITAL READINESS SELF-ASSESSMENT CHECKLISTS



How to complete the Checklist

Digital readiness evaluates the institution's foundational digital capacity across three specific domains namely **people**, **processes** and **technology**. It is not just about the availability of technology, but also about the institution's ability to plan, manage, and sustain digital transformation over sustained periods of time without donor intervention or support.

The color coding and maturity levels are intended to help institutions identify actions that are foundational, intermediate, or more advanced. Institutions at an early stage of digital development may begin with lower-maturity actions, while institutions with stronger capacity may engage progressively with medium- and high-maturity actions.

Although the checklist is structured around **Yes/No** responses for simplicity and accessibility, digital readiness should not be understood as a purely binary concept. In practice, many institutions may find that some areas are only partially in place, still evolving, or unevenly applied across the organization. The purpose of the checklist is therefore to support reflection, discussion, and institutional learning, rather than to provide a definitive measure based solely on a simple yes or no answer. Used in this way, the checklist can help institutions identify strengths, highlight gaps, and encourage more informed planning for digital transformation.

TIP

Institutions that have previously undertaken the NHRI Capacity Assessment may find it useful to use the findings as they will inform the digital readiness assessment. Areas identified as institutional capacity gaps, such as governance, human resources, or strategic planning, may also influence digital readiness and implementation.

3.1 PEOPLE – SKILLS, ROLES, AND LEADERSHIP

The availability of skilled technical resources within or available to the institution. Without the correct skillsets, institutions are unable to sustain systems over the long term, meaning system sustainability is very much compromised. Without the required skills, systems have no longevity or business continuity.






CONSIDERATION	YES / NO	SUGGESTED NEXT STEPS	NOTES
1. Is NHRI leadership supportive of digital transformation? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Issue a short “Digital Commitment” note signed by leadership. ↳ Set 3-5 clear digital goals for the next 6 months.	
2. Are responsibilities for digital transformation clearly defined? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Assign a “Digital Champion” or team lead. ↳ Add digital duties to job descriptions and staff evaluations.	
3. Do staff have basic digital skills ⁱ and access to tools (email, office apps, secure messaging)? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Run a staff survey to assess baseline skills. ↳ Provide email/office apps/ secure messaging to all. ↳ Offer short training sessions on key tools (email, security, accessibility).	
4. Is there an ICT or innovation focal point? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Nominate a staff member or hire an ICT Officer. ↳ Publish duties and responsibilities of the ICT focal point.	
5. Does each department have a digital focal point? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Identify one person per department. ↳ Hold brief weekly or monthly check-ins to share progress and challenges.	
6. Is there a staff training plan for digital tools and data security? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Develop a 6-month basic training plan covering computer use, privacy, and digital workflows.	

ⁱ Basic digital skills would equate to a person having the skills to navigate microsoft on a personal computer, or a person making use of a smartphone.

<p>7. Do staff have regular access to computers, laptops, or mobile devices?</p> <p><input type="radio"/> Yes <input type="radio"/> No</p> <p>● ● ●</p>	<p>↳ Define minimum ICT needs and plan for gradual procurement.</p>	
<p>8. Are there personnel trained in legal data protection and digital rights?</p> <p><input type="radio"/> Yes <input type="radio"/> No</p> <p>● ● ●</p>	<p>↳ Introductory workshop on lawful basis of data usage, minimization and retention of data as well as record management.</p>	
<p>9. Are staff aware of the opportunities and risks associated with Artificial Intelligence (AI) in digital systems?</p> <p><input type="radio"/> Yes <input type="radio"/> No</p> <p>● ● ●</p>	<p>↳ Provide introductory training on AI capabilities, limitations, and ethical considerations.</p> <p>↳ Ensure staff understand that AI tools should support investigations and analysis but not replace human judgement.</p> <p>↳ Build awareness of risks such as bias, incorrect outputs, and data protection concerns.</p>	

3.2 PROCESSES – PLANNING, GOVERNANCE, AND PROJECT MANAGEMENT

Process readiness refers to the existence and clarity of institutional workflows that guide task execution. For example, a well-defined manual procedure for archiving documentation for a specified duration demonstrates foundational structure. Effective digitization builds on such established processes, ensuring that digital systems replicate and improve upon existing procedural logic.

CONSIDERATION	YES / NO	SUGGESTED NEXT STEPS	NOTES
1. Is there a clear digital roadmap ⁱⁱ or plan? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Create a simple roadmap with phases, goals, and responsible persons. ↳ Review progress monthly.	
2. Are any internal processes currently digitalized? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Pick one low-risk process to digitize (pilot); define entry/exit criteria. ↳ Scale to two more units after lessons learned; measure cycle-time impact.	
3. Is there a project manager or team for ICT initiatives? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Appoint a project lead and clarify their role.	
4. Is there a functioning helpdesk or IT support mechanism in place to handle current system issues? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Publish a support email/phone and their operational hours; designate a focal point.	
5. Are digital consent and user privacy protocols in place? 	<input type="radio"/> Yes <input type="radio"/> No	↳ Add plain-language consent text to all forms where applicable. ↳ Capture time date stamped electronic consents in digital systems, add a consent log and capture log files in systems that are operational. ↳ On client facing systems include links to Data Protection laws/regulations. Clearly defining personal data usage, data accessing, and usage.	

ii A digital roadmap is defined by a 5-year forward plan which describes the technology delivery plan with associated milestones.

<p>5. Are project steps and deliverables defined (e.g., milestones, outputs)?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Use a simple plan (e.g., start, design, develop (inhouse dev)/deploy (OTS) and test, implement, review).</p>	
<p>6. Is a phased or step-by-step approach used for new systems?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Avoid “big-bang” launches—test and scale gradually.</p>	
<p>7. Are change management and communication plans in place?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Inform all staff before and during major ICT changes.</p> <p>↳ Collect feedback regularly.</p>	
<p>8. Is risk management considered?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ List possible risks (e.g., data loss, power cuts) and plan how to respond.</p>	
<p>9. Are complaint and redress mechanisms defined for digital data breaches?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Write a 2-page breach response SOP (who, when, how); create a contact list.</p>	
<p>10. If AI tools are used or planned, are governance rules and human oversight mechanisms defined?</p> <p> </p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Define acceptable uses of AI within NHRI systems.</p> <p>↳ Ensure automated outputs are subject to human review before decisions are taken.</p> <p>↳ Document how AI tools are integrated into workflows and accountability structures.</p>	

3.3 GOVERNANCE – LEGAL AND POLICY FRAMEWORK

Alignment with National ICT and Public Sector Digital Policies

Part 1

Part 2

Part 3

Annex 1

Annex 2

CONSIDERATION	YES / NO	SUGGESTED NEXT STEPS	NOTES
<p>1. Are there national data protection or privacy laws that apply to your NHRI (for collection, processing, storage and sharing of personal data)?</p> <p>● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Maintain a register of how personal data is collected, used, stored, and shared, and ensure that staff receive training on privacy and data protection responsibilities.</p> <p>↳ Review relevant laws, policies, and current practices, and assign clear responsibility for privacy oversight within the institution.</p> <p>↳ Keep records to support accountability and ongoing review.</p>	
<p>2. Are data handling and consent procedures in place and followed?</p> <p>● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Publish clear guidance explaining how personal data is collected, used, stored, and how individuals may withdraw consent or exercise their rights.</p> <p>↳ Maintain a record of data access, correction, or deletion requests and ensure that these are handled consistently and appropriately.</p> <p>↳ Institutions operating at a higher level of digital maturity should go further by automating data retention controls and undertaking regular compliance reviews.</p>	
<p>3. Is there Freedom of Information (FOI) or access-to-information laws that affects how the NHRI shares data?</p> <p>● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Identify and review the laws, policies, and rules governing the sharing of information, and ensure that staff are trained on what information may be disclosed, to whom, and under what conditions.</p> <p>↳ Put in place clear internal guidance to support consistent decision-making and lawful information sharing.</p>	



<p>4. Are electronic records, e-signatures, and digital evidence legally accepted?</p> <p>●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p> <p>↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by publishing regular transparency reports and strengthening formal disclosure monitoring and accountability mechanisms.</p> <p>↳ Confirm the legal status and admissibility of electronic signatures and records and implement approved e-signature solutions for relevant processes.</p> <p>↳ Maintain appropriate backup arrangements where required and keep logs, metadata, or other records that demonstrate the authenticity, integrity, and traceability of electronically signed documents (IE DocuSign).</p> <p>↳ Institutions operating at a <i>more advanced mature level</i> should go further by strengthening auditability and advocating for broader legal and institutional recognition of electronic transactions where gaps remain.</p>	
<p>5. Are there laws or policies on ICT procurement, open-source software, or cloud storage?</p> <p>● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p> <p>↳ Identify and review the laws, standards, and policy requirements that apply to procurement, digital systems, and related technologies, and ensure that procurement decisions are aligned with these requirements.</p> <p>↳ Apply these standards consistently when selecting, acquiring, or contracting for systems and services.</p> <p>↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by conducting regular compliance reviews and advocating for secure, interoperable, and open systems where appropriate.</p>	

<p>6. Are national cybersecurity and cloud-use frameworks followed?</p> <p>● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Review the national cybersecurity policy and align internal rules, procedures, and practices with its requirements and expectations.</p> <p>↳ Ensure that relevant staff understand these obligations and that they are reflected in day-to-day operations and governance arrangements.</p> <p>↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by reviewing compliance on a regular basis and formally reporting cybersecurity risks and gaps to management.</p>	
<p>7. Are there formal governance bodies or working groups for digital transformation that include the NHRI?</p> <p>●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Identify the relevant national digital, ICT, data governance, or cybersecurity committees and coordination structures, and take steps to engage with them through observer status, membership, or other appropriate participation mechanisms.</p> <p>↳ This should help ensure that the institution remains informed and able to contribute to discussions that affect its mandate and digital development.</p> <p>↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by actively contributing expertise, sharing lessons learned, and promoting good practice in relevant national forums.</p>	

3.4 TECHNOLOGY – TECHNICAL REQUIREMENTS FOR A SAFE AND SECURE SYSTEM

Effective digital transformation relies heavily on the use of technology that is appropriate, secure, and sustainable. NHRIs must ensure that their hardware, software, and digital infrastructure are aligned with their institutional size, mandate, and relevant legal and ethical frameworks. The selected system architecture should also incorporate necessary security components and reflect the institution’s operational requirements, including whether to deploy off-the-shelf solutions or in-house developed systems.

Is the institution technically ready for digital transformation. Does it have the technical resource and capacity to deliver a robust sustainable digital service and system that is sustainable over the medium- to long-term.

CONSIDERATION	YES / NO	SUGGESTED NEXT STEPS	NOTES
A. Core Infrastructure and Connectivity			
1. Is the NHRI’s network available, stable, and secure? 	<input type="radio"/> Yes <input type="radio"/> No	<ul style="list-style-type: none"> ↳ Address basic connectivity challenges. ↳ Establish a simple, functional network environment, whether through improved internet access, better internal connectivity, or a basic local area network. ↳ Ensure that the network setup is reliable enough to support essential operations and that staff understand how to use it at a basic level. ↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by monitoring network performance, documenting network arrangements, and progressively strengthening security through measures such as firewalls, network segmentation, and regular security review. 	
2. Is ICT infrastructure functional and scalable? 	<input type="radio"/> Yes <input type="radio"/> No	<ul style="list-style-type: none"> ↳ Identify key infrastructure bottlenecks and take practical steps to align basic infrastructure with the institution’s immediate digital needs and priorities. ↳ Focus on establishing the minimum equipment, connectivity, and system capacity required to support essential digital functions. 	

3. Has the NHRI selected a digital infrastructure architecture (cloud, on-premises/ hybrid)?



- Yes
- No

↳ Institutions operating at a higher level of digital maturity should go further by planning for scale-up, introducing virtualization where appropriate, and adopting more scalable solutions such as cloud-based or other flexible systems, with regular capacity reviews.

↳ Understand the basic differences between cloud-based and on-premises solutions, and assess their advantages, limitations, jurisdictional concerns, costs, risks, and suitability in relation to the institution's needs and the national digital strategy.

↳ Use this analysis to inform a clear and justified infrastructure decision.

↳ Institutions operating at a higher level of digital maturity should go further by formally documenting this decision and reviewing associated risks, costs, compliance requirements, and sustainability on a regular basis.

4. Are digital systems accessible remotely and mobile-friendly?



- Yes
- No

↳ Ensure that staff have reliable mobile access and secure remote connectivity where required and strengthen this through appropriate controls such as multifactor authentication and other access safeguards.

↳ This should support continuity of work while protecting systems and data from unauthorized access.

↳ Institutions operating at a *higher level of digital maturity* should go further by expanding mobile-enabled service options where appropriate.

↳ Monitoring the performance, reliability, and security of remote access arrangements on a regular basis.

B. Equipment, Power, and Connectivity

5. Do all service locations have electricity?



- Yes
- No

- ↳ Conduct basic readiness assessments to gather information, about electricity availability, network connectivity, and the number and condition of devices available for use.
- ↳ Use this information to identify and address the most immediate gaps in power, network access, and equipment needed to support basic digital operations.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by tracking readiness more systematically and, before any system go-live, completing a service readiness checklist and establish clear go/no-go criteria for each intended deployment site.

6. Do all locations have reliable internet access and back-up connections?



- Yes
- No

- ↳ Assess and monitor the reliability of electricity, connectivity, and device availability across offices and service locations.
- ↳ Take steps to strengthen these through improved infrastructure, backup arrangements, and more consistent operational support.
- ↳ This should help ensure that digital services can function more reliably across the institution.
- ↳ Institutions operating at a higher level of digital maturity should go further by validating site readiness on a regular basis and maintaining up-to-date readiness records to support planning, maintenance, and deployment decisions.

7. Are there enough laptops or tablets for staff?



Yes

No

- ↳ Assess the availability and distribution of devices across the institution and work progressively towards ensuring that each staff member who requires digital access has reliable access to an appropriate device.
- ↳ Reduce excessive device sharing and plan allocation in line with operational needs and staff roles.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by establishing structured device lifecycle management and regular replacement plans to ensure continued reliability, performance, and security.

8. Are devices and networks protected with antivirus and firewalls?



Yes

No

- ↳ Put in place and maintain essential endpoint security measures, including antivirus protection, updated firewalls, and consistent patching and update practices across institutional devices.
- ↳ Move toward more centralized security and update management so that protections are applied consistently and monitored more effectively across the environment.
- ↳ Institutions operating at a higher level of digital maturity should go further by implementing advanced endpoint protection, such as Endpoint Detection and Response (EDR), in a manner aligned with recognized good practice and standards, including NIST and ISO frameworks, embedded within sound ICT governance arrangements.

9. Is there secure physical space for on-premises server hosting, if used?



Yes

No

↳ Identify a secure room or controlled area where critical ICT equipment, servers, or network devices can be kept with restricted physical access.

↳ Put in place the most basic environmental and security measures needed to protect equipment from unauthorised access, damage, or disruption.

↳ Institutions operating at a *higher level of digital maturity* should go further by applying more formal data-centre standards, including cooling and access controls, and, where appropriate, using certified or tiered hosting facilities.

C. Security, Maintenance and Sustainability

10. Is there a regular device maintenance and replacement policy?



Yes

No

↳ Establish and apply an Information Technology lifecycle management approach that includes maintaining an inventory of equipment, tracking maintenance needs, and monitoring servicing and replacement schedules. This should help ensure that devices remain functional, secure, and fit for purpose over time.

↳ Institutions operating at a *higher level of digital maturity* should go further by using usage, performance, and maintenance data to inform planned replacement cycles and longer-term asset management decisions.

11. Is secure access available for remote workers (VPN, MFA,¹³ etc.)?



Yes

No

↳ Provide secure remote access to institutional systems, including the use of VPN access where appropriate, and strengthen this through measures such as multifactor authentication and encryption. This should help ensure that staff can work remotely while maintaining the security and confidentiality of institutional systems and data.

12. Are backups and disaster recovery plans in place?



- Yes
- No

↳ Institutions operating at a *higher level of digital maturity* should go further by enforcing formal secure remote-working standards and actively monitoring compliance and access risks.

↳ Put in place reliable backup arrangements for critical data and systems, and regularly test data restoration to ensure that backups are complete, usable, and available when needed. This should help the institution maintain continuity and recover important information in the event of system loss, corruption, or system failure.

↳ Institutions operating at a *higher level of digital maturity* should go further by maintaining and regularly testing a full disaster recovery plan that supports broader service continuity and resilience.

13. Are hosting and data storage decisions documented?



- Yes
- No

↳ Make a clear and informed decision on where institutional data is stored, and ensure that storage arrangements comply with applicable legal, regulatory, and policy requirements. This should include confirming that data is held in a manner that supports security, confidentiality, access control, and accountability.

↳ Institutions operating at a *higher level of digital maturity* should go further by regularly reviewing hosting-related risks, contractual arrangements, data residency implications, and ongoing compliance obligations to ensure that storage arrangements remain appropriate, secure, and sustainable over time.

D. Software & New Systems

14. Has the NHRI decided whether to build or buy software?



- Yes
- No

- ↳ Compare the basic costs, resource implications, and internal capacity required for different options, and use this to identify the most practical and affordable approach for the institution's current needs.
- ↳ Focus on understanding what can realistically be supported with existing resources and where immediate constraints exist.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by piloting suitable options and ensuring that contractual arrangements allow sufficient flexibility, scalability, and adaptability over time.

15. Is the institution considering the use of Artificial Intelligence (AI) within digital systems (e.g., complaint triage, analytics, document summarization)?



- Yes
- No



- ↳ Assess potential AI use cases carefully and understand the associated risks, limitations, and safeguards before adoption.
- ↳ Where appropriate, pilot AI tools cautiously in clearly defined areas, ensuring strong data protection measures, human oversight, and controlled use throughout the piloting phase.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by implementing formal AI governance policies, bias and performance monitoring, and audit mechanisms for AI-supported processes.

16. Is internal capacity available to maintain systems?



- Yes
- No

- ↳ Identify technical skills gaps relevant to the institution's digital systems and priorities, and address these through targeted staff training, external support, or recruitment where feasible.
- ↳ Build sufficient technical capacity to support the operation, maintenance, and improvement of digital systems.

		<p>↳ Institutions operating at a <i>higher level of digital maturity</i> should, if applicable, maintain stronger in-house technical expertise to provide sustained support, oversight, and continuous improvement.</p>	
<p>17. Has open-source software been considered? </p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>	<p>↳ Shortlist both open-source and proprietary options and assess them against the institution’s functional, technical, financial, and operational requirements.</p> <p>↳ Pilot suitable options where feasible and use the results to inform a balanced selection decision. Institutions should avoid vendor lock-in and ensuring that contracts, architectures, and implementation arrangements support interoperability, portability, and clear exit strategies.</p>	
<p>18. Is the envisaged software going to be developed in-house? </p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>	<p>↳ Identify the basic skills, roles, tools, and support needed to undertake software development or system configuration activities in a controlled manner.</p> <p>↳ Focus on understanding the minimum internal and external capacity required before development work begins.</p> <p>↳ Institutions operating at a <i>higher level of digital maturity</i> should go further by defining clear Software Development Life Cycle (SDLC) stages and governance arrangements, and ultimately applying a SDLC supported by appropriate quality assurance, testing, documentation, and security controls.</p>	

19. Is the institution considering a hybrid (paper and digital) solution?



Yes

No

↳ Identify which processes remain paper-based and assess where manual practices continue to be necessary, feasible, or legally required.

↳ Use this understanding to begin planning a realistic and phased transition toward digital processes, taking into account operational needs and readiness constraints.

↳ Institutions operating at a *higher level of digital maturity* should go further by securing stakeholder buy-in, defining clear transition timelines, and managing the shift from paper-based to digital processes in a structured and well-communicated manner.

E. AI, Automation and Emerging Technologies

20. Has the NHRI assessed whether any AI-enabled tools are appropriate for its mandate and operational needs?



Yes

No

↳ Identify potential low-risk AI use cases, such as translation, transcription, document search, summarisation, or administrative support, and assess their suitability, value, and risks against institutional needs, legal obligations, and operational realities.

↳ Any consideration of AI should remain practical, proportionate, and aligned with the institution's mandate and capacity.

↳ Institutions operating at a higher level of digital maturity should go further by maintaining a documented AI use-case register that distinguishes approved, restricted, and prohibited uses, supported by periodic reviews.

21. Are there rules or internal controls governing the procurement or use of AI-enabled tools?



Yes

No

- ↳ Record any AI tools already being used by staff and issue clear interim guidance on acceptable use.
- ↳ Develop and approve minimum rules for AI procurement, testing, use, and oversight, including approval requirements for new tools and clarity on roles and responsibilities.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by maintaining a formal AI governance framework covering procurement, vendor due diligence, human oversight, accountability, auditability, and periodic reviews.

22. Is sensitive data protected when AI tools are used?



Yes

No

- ↳ Prohibit the input of sensitive personal, case-related, or confidential information into unapproved public AI tools, and define clearly what data may and may not be used in approved AI systems.
- ↳ Apply appropriate privacy, security, and access controls to any authorised AI tools to ensure that data is handled safely and lawfully.
- ↳ Institutions operating at a higher level of digital maturity should go further by conducting formal privacy and risk assessments for AI-enabled systems, putting in place contractual safeguards, and monitoring compliance on a regular basis.

23. Is human oversight applied to AI-assisted outputs and decisions?



Yes

No

↳ Require staff to review AI-generated outputs before they are used, shared, or acted upon, and define clearly which outputs or decisions must always be subject to human validation, particularly where complaints, investigations, recommendations, or rights-related matters may be affected.

↳ This should help ensure that AI-assisted processes remain accountable and do not replace human judgement in sensitive areas.

↳ Institutions operating at a *higher level of digital maturity* should go further by maintaining documented *human-in-the-loop* review points, escalation procedures, and clear accountability arrangements for AI-assisted workflows.

24. Are AI tools assessed for accuracy, bias, reliability, and explainability?



Yes

No

↳ Test AI-generated models and generated outputs from models for obvious inaccuracies before operational use and introduce simple quality checks to assess accuracy, consistency, and potential bias.

↳ These checks should help ensure that AI-assisted outputs are reliable enough for the context in which they are being used and that obvious risks are identified early.

↳ Institutions operating at a *higher level of digital maturity* should go further by establishing regular testing, monitoring, and documentation of AI performance, bias risks, and known limitations, together with corrective actions where needed.

F. Hardware (on premises)

25. Are current computers, servers, and networking equipment sufficient for digitization needs?



- Yes
- No

- ↳ Assess baseline infrastructure capacity, including processing power, memory, storage, and input/output performance, and address obvious bottlenecks that may affect system reliability or performance.
- ↳ Plan for system scale-up or system scale-out as demand grows, introduce virtualization where appropriate, and build in sufficient headroom to support expected growth.
- ↳ Institutions operating at a higher level of digital maturity should go further by adopting more scalable architectures, including cloud-based or autoscaling solutions where feasible.
- ↳ Conduct regular capacity reviews to support performance, resilience, and future planning.

26. Are hardware systems scalable, virtualized, or cloud-compatible?



- Yes
- No

- ↳ Review the institution's current hardware environment to determine whether it can support future growth, changing system demands, and more flexible deployment models.
- ↳ Identify opportunities to improve efficiency and resilience through virtualization or more adaptable infrastructure planning, and ensure that future investments do not limit the institution's ability to move toward cloud-based or hybrid solutions if needed.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by implementing more flexible and scalable infrastructure models.
- ↳ Review infrastructure suitability on a regular basis.

G. Data Protection, monitoring and accessibility

27. Is data encrypted when at rest (stored in the database) and in transit (over the network)?



- Yes
 No

- ↳ Ensure that encryption is enabled for sensitive data and progressively strengthen this by applying encryption to databases, backups, and other critical data stores.
- ↳ This should help protect institutional information from unauthorized access, loss, or compromise both during transit, in storage and in recovery.
- ↳ Institutions operating at a *higher level of digital maturity* should go further by implementing secure key management practices and stronger controls over the generation, storage, rotation, and protection of encryption keys if utilized.

28. Are multifactor authentication (MFA) and role-based access controls used?



- Yes
 No

- ↳ Strengthen access security by enforcing strong password practices, using secure remote access arrangements such as VPNs where appropriate, and applying multifactor authentication for access to systems with sensitive information.
- ↳ Access rights should also be reviewed regularly to ensure that they remain appropriate to staff roles and responsibilities.
- ↳ Institutions operating at a higher level of digital maturity should go further by adopting more advanced access control approaches, such as zero-trust principles and anomaly monitoring, to detect and respond to unusual or unauthorized access activity.

29. Is cybersecurity infrastructure current and compliant?



- Yes
 No

- ↳ Upgrade or replace redundant cybersecurity.
- ↳ Compliance to cybersecurity is of utmost importance as must form part of your ICT best practice guidelines.
- ↳ Cybersecurity guidelines must be adhered to.

30. Are safeguards in place to prevent sensitive complaint data from being shared with external AI systems without proper agreements?



- Yes
 No

↳ Ensure that staff do not upload sensitive complaint, case-related, or confidential information into external AI tools. Additionally, implement clear policies governing the use of AI tools and third-party APIs. These policies should define acceptable use, data handling requirements, approval processes, and safeguards for protecting institutional and personal information.

↳ Institutions operating at a higher *level of digital maturity* should go further by establishing formal data processing agreements and implementing privacy-preserving AI configurations and controls aligned to Data Protection Laws.

31. Are antivirus, firewalls, and endpoint protection systems deployed and maintained?



- Yes
 No

↳ Ensure that antivirus, firewall, and endpoint protection measures are deployed across institutional devices and systems, and that they are regularly updated, monitored, and maintained.

↳ Strengthen consistency by centralizing security management where feasible, so that protection, patches, and alerts can be applied and reviewed across the environment in a more coordinated manner.

↳ Institutions operating at a *higher level of digital maturity* should go further by implementing more advanced endpoint protection and detection capabilities, supported by formal monitoring, incident response, and alignment with recognized cybersecurity standards and good governance practices.

32. Are systems monitored for errors and performance?



- Yes
- No

- ↳ Review basic system logs on a regular basis and establish alerts for failures, errors, or other significant events that may affect the availability, security, or performance of systems. This should help the institution detect problems quicker, allowing for responses to be done in a timely and coordinated manner.
- ↳ Institutions operating at a higher *level of digital maturity* should go further by using dashboards, reporting tools, and more structured monitoring arrangements to support ongoing oversight, analysis, and decision-making.

33. Do systems meet accessibility and inclusion standards?



- Yes
- No

- ↳ While ensuring that traditional manual processes remain available, digital systems and services should be accessible on mobile devices.
- ↳ Functioning reliably for users with limited connectivity or low-bandwidth access. This will help improve access, continuity, and inclusion for staff and rights-holders operating in different connectivity environments.
- ↳ Institutions operating at a higher level of digital maturity should go further by aligning digital services with recognized accessibility standards, including WCAG ([Web Content Accessibility Guidelines](#)), to support more inclusive and equitable access.

CONSIDERATION	YES / NO	SUGGESTED NEXT STEPS	NOTES
<p>1. Is a dedicated ICT/ digital innovation budget or discretionary funding available for digitization efforts?</p> <p>● ● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Establish a basic ICT line item within the institutional budget and begin with low-cost, high-impact digitization initiatives, such as digitizing priority manual processes.</p> <p>↳ Build an internal business case that links digital investment to improved service delivery, operational efficiency, and institutional effectiveness. Institutions operating at a higher level of digital maturity should go further by formalizing the digital budget within annual planning cycles, introducing prioritization criteria for digital projects, allocating limited funding for pilots and proof-of-concept initiatives, and ultimately maintaining a multi-year digital investment plan aligned with strategic objectives and reviewed for impact over time.</p>	
<p>2. Are any other funds (donor or international technical assistance) available to support system development, training, or infrastructure?</p> <p>● ● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>	<p>↳ Identify potential donors and technical partners whose priorities align with human rights, governance, and institutional strengthening, and prepare concept notes focused on foundational systems, basic digital infrastructure, and capacity building.</p> <p>↳ Designate a focal point to coordinate donor and partner engagements and to help ensure that support is aligned with institutional needs.</p>	

<p>3. Does the institution have internal financial governance mechanisms that allow for agile procurement, rapid prototyping, and system upgrades?</p> <p>● ● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p> <p>↳ Review procurement and financial rules to identify bottlenecks that delay or constrain ICT projects, and develop simpler procedures for low-value or pilot digital initiatives where possible.</p> <p>↳ Build awareness among finance and procurement staff of the practical requirements of digital projects so that basic ICT needs can be supported more effectively.</p> <p>↳ Institutions operating at a higher level of digital maturity should go further by introducing more flexible procurement arrangements, strengthening collaboration between ICT, finance, and procurement units, and progressively enabling more agile approaches that support upgrades, security improvements, and ongoing system development.</p>	
<p>4. Are long-term budgets allocated for system hosting, support, and upgrades?</p> <p>● ● ●</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p> <p>↳ Identify existing systems that have unfunded operational or maintenance costs, and ensure that basic recurring expenses such as hosting, support, and licensing are included in annual budgets.</p> <p>↳ Raise awareness of system lifecycle costs during planning and procurement so that digital investments are not treated as one-off expenses.</p>	

↳ Institutions operating at a *higher level of digital maturity* should go further by introducing multi-year budgeting for core systems and infrastructure, funding routine maintenance and upgrades, tracking total cost of ownership, and progressively integrating lifecycle costing into wider financial and strategic planning.

Part 3

DIGITAL SOLUTIONS FOR NHRIS

This section of the document sets out practical solution pathways for an NHRI. The chosen pathway depends on the NHRI's digital maturity, resources and national context. This section helps NHRIs translate the self-assessment results into solution choices.

NOTE

Decisions on digital solutions should be aligned with the broader institutional priorities identified through strategic planning processes, including findings from the NHRI Capacity Assessment where available.

1. OVERVIEW OF SOLUTION PATHWAYS

Three main pathways are available for NHRIs:

- ↳ **off-the-shelf solutions** (including open-source packages that can be deployed “as is”), and
- ↳ **in-house, internally** developed bespoke solutions, often open source.
- ↳ **Hybrid solution** combines off-the-shelf systems with bespoke or internally developed components.

Table 5 **Solutions Comparison table**

DIMENSION	OFF-THE-SHELF SOLUTIONS	BESPOKE / OPEN-SOURCE	HYBRID SOLUTION
Time to deploy	Fast	Slower	Medium
Customisation	Limited	High	Medium-High
Required digital maturity	Low-Medium	Medium-High	Medium
Vendor dependency	Medium-High	Low	Medium
Data sovereignty	Depends on vendor	High	Medium-High
Long-term flexibility	Medium	High	High

A.**What are off-the shelf solutions?**

Off-the-shelf solutions are pre-built, proven software platforms, which are either open-source distributions or closed source commercial products. These solutions can be configured to NHRI workflows and deployed quickly without custom development. In many instances they provide ready-made capabilities and associated functionality covering the following areas:

- ↳ **Complaints & investigations** (intake, triage, workflows, evidence, audit, documentation of human rights violations)
- ↳ **Document & knowledge management** (structured libraries, tagging, search, publication)
- ↳ **Monitoring (Optional Protocol to the Convention Against Torture/National Prevention Mechanism)** via mobile data capturing and dashboards
- ↳ **UPR/Treaty tracking** (recommendations, actions, indicators, reporting)
- ↳ **Analytics & security** (dashboards, role-based access, logging)

Examples of such solutions include [Uwazi](#)¹⁴(HURIDOCS) for case and document libraries. [ODK](#)¹⁵ and [Kobo Toolbox](#)¹⁶ for field data collection making use of small handheld devices. [IMPACT OSS](#)¹⁷ for recommendations tracking, and commercial solutions such as Microsoft Dynamics 365 for configurable supported case management.

B.**When are off-the-shelf solutions a good fit?**

Off-the-shelf solutions are most suitable when:

- ↳ Digital maturity is low to medium
- ↳ Speed and donor timelines matter
- ↳ Internal technical capacity is limited
- ↳ Standard workflows are acceptable

Often, management chooses **off-the-shelf systems** because they deliver faster *time-to-value* solutions. Generally offering proven workflows that reduce delivery risks and suit donor milestones, supported by an ecosystem of technical resources, detailed training, and documentation. However, it is important to weigh up the risks; off-the-shelf options require a capable support partner or an internal technical skills set for maintenance, updates and security. Furthermore, commercial off-the-shelf platforms entail ongoing licensing potential vendor lock-in, high solution customization costs and data integration constraints.

14 HURIDOCS, 'Uwazi Platform Features', HURIDOCS, n.d.

15 Open Data Kit, 'Open Data Kit (ODK)', Open Data Kit, n.d.

16 KoBoToolbox, 'KoBoToolbox', KoBo Inc., Cambridge, n.d.

17 Impact Open Source Software Trust, 'IMPACT OSS', Impact Open Source Software Trust, n.p., n.d.

A.**What is a bespoke NHRI system?**

An internally developed bespoke NHRI system is a tailored solution designed making use of proven open-source components. These systems are designed to meet specific requirements and focus on featured functionality that conforms to the exact NHRI's mandate, associated languages, and defined processes.

Rather than buying a single suite, the institution (in some instances with partners or other government agencies) opt to design a best-of-breed module or modules to meet their specific NHRI requirements under its own governance and roadmap.

Building an internal open-source bespoke system (both open source and closed source) can potentially offer NHRIs with a cost-effective, adaptable, and sustainable system, however it comes with its risks. While the pathway to developing secure, customized digital systems for operations like case tracking, case monitoring, information management, data monitoring, and reporting requires a high level of digital maturity.

Bespoke systems are suitable when:

- ↳ Digital maturity is **medium to high**
- ↳ Data sovereignty is critical
- ↳ Mandate-specific workflows are required
- ↳ Long-term flexibility outweighs speed

B.**When are bespoke solutions a good fit?**

Management generally opts for an internally developed, open-source solution when control and sovereignty over data, system features, and the digital roadmap is of national importance. Additionally, they opt for internally developed solutions when fit-for-purpose solutions are required to meet specific NHRI needs and workflows as well as when an NHRI is cost sensitive (less license exposure, more investment in skills and targeted support). Furthermore, when sustainability through the adoption of open standards and portability is a priority to avoid long-term vendor lock-in, internally designed and developed solutions are seen as the only option.

The development of bespoke solutions is not without its risks, capacity dependence on a strong product owner and technical skills (in-house or retained) are just a few risks that need to be considered. A longer time to value is often associated with internally developed bespoke solutions, requiring disciplined lifecycle management ensuring that scope creep does not happen.

A.**What is a hybrid solution?**

A hybrid solution combines off-the-shelf systems with bespoke or internally developed components to create a digital environment that is better aligned to the NHRI's specific needs. Rather than relying entirely on a single pre-built platform or developing everything from scratch, the institution adopts a selective approach, using proven existing tools where they are fit for purpose, while developing or configuring additional components where greater flexibility or localization is required.

For example, an NHRI may use an off-the-shelf solution for document management, data collection, or helpdesk functions, while developing a bespoke case management module, analytics dashboard, integration layer, or reporting component tailored to its mandate and workflows. In this way, the hybrid approach allows the institution to benefit from the speed and reliability of established solutions while still retaining flexibility in areas where customization is important.

A hybrid approach can be particularly useful where an NHRI wants to improve services incrementally, manage costs over time, or avoid over-dependence on a single vendor or technology stack. However, this model also requires careful planning to ensure that the different components work well together, that data can be shared securely across systems, and that governance, support, and maintenance responsibilities are clearly defined.

Hybrid solutions are suitable when:

- ↳ Some needs can be met by **off-the-shelf tools**, while others require **custom features**.
- ↳ The NHRI needs **speed of deployment with flexibility**.
- ↳ The institution wants to **avoid full vendor dependency**.
- ↳ The NHRI plans to **grow systems gradually as capacity improves**.

B.**When is a hybrid solution a good fit?**

A hybrid solution is often a good fit when an NHRI needs a balance between **speed of deployment, flexibility, and long-term sustainability**. It may be suitable where some institutional needs can be met through existing proven tools, while other functions require custom development to reflect national legal requirements, internal workflows, language needs, reporting obligations, or integration with external government systems.

Management may also consider a hybrid approach when budget constraints make it impractical to develop a full bespoke solution from the outset, but where a purely off-the-shelf model would not sufficiently meet operational requirements. In such cases, the institution can start with selected pre-built systems and gradually introduce bespoke modules as digital maturity, technical capacity, and resources increase.

The hybrid model can offer significant advantages, but it also requires disciplined technical governance. Institutions should pay close attention to interoperability, data standards, cybersecurity, vendor management, lifecycle support, and overall architectural coherence. Without proper planning, hybrid environments can become fragmented or difficult to maintain. Where well governed, however, a hybrid solution can provide a practical and scalable route to digital transformation.

2. TECHNICAL REQUIREMENTS BASED ON THE SOLUTION PATHWAY

This section elaborates on the technical requirements to implement the respective solutions and is intended for IT teams supporting the NHRI's digital development.

2.1 OFF-THE-SHELF NHRI SYSTEM

A.

What it requires

An off-the-shelf solution is a pre-built software product either commercial or a packaged open-source systems adopted by configuration and installation, not coding. It delivers standard NHRI capabilities out of the box and therefore requires implementation only (no custom development). Additionally, product selection, configuration of workflows, data migration, necessary integrations (where applicable), user training, and ongoing operations are generally supplied by the vendors. Costing of such solutions relate to licences, system implementations, hosting, as well as training and ongoing support. To that end the following applies to off-the-shelf solutions:

Key roles (Some of these roles may be fulfilled by the same individual.)

- ↳ **Executive Sponsor:** owns scope and priorities, accepts configured features against NHRI requirements.
- ↳ **Project Lead:** plans delivery, budget, timelines and risks as well as coordinates with the institution's technical resources.
- ↳ **Business Process Analysis:** documents the institutions requirements, maps the requirements to the system purchased.
- ↳ **Platform/System Administrator:** day-to-day configuration, permissions, system releases, system housekeeping and maintenance.
- ↳ **Integration:** implements system components, data migration, and interfaces to legacy systems.
- ↳ **Security & Compliance:** manages all security components, audits, and data controls.
- ↳ **Testing & User Acceptance Testing (UAT):** orchestrates user testing; verifies that configured processes meets the NHRI's requirements as per the Business Requirements Specification (BRS).
- ↳ **Training & Support:** produces user and admin guides, runs training and assists with system handover.

Technology (essentials)

- ↳ **Platform:** the off-the-shelf system/solution that meets the specific requirements of the NHRI.
- ↳ **Infrastructure:** Cloud or On-Premises technology. Associated infrastructure if On-Prem is opted for.
- ↳ **Foundations:** identity/ Single Sign-On (SSO), access control (RBAC/ User Based Access Control, UBAC), audit logging, monitoring/alerting, **backup and restore procedures**, and data-residency settings.

Processes

- ↳ **Training & user support:** role-based curricula; user/admin manuals; onboarding and refresher training.
- ↳ **ICT governance & best practice:** the various ICT governance frameworks and ICT best practices that are used to manage ICT in the organisation.
- ↳ **Data protection and security SOPs:** Quality Assurance (QA) checklists; UAT and go-live gates; DPIA and retention where applicable.

Financial Requirements for off-the-shelf NHRI systems

While the implementation has lower build effort, the costs associated with off-the-shelf systems/solutions comes in the form of **subscriptions or product licencing costs**. Maintenance and support however remain ongoing and is certainly comparable in cadence to bespoke systems/solutions. Therefore, to ensure one focuses correctly on the financial aspects, up-front and recurring line-item costs are listed below, which are directly linked to off-the-shelf systems/solutions:

- ↳ **Licensing & subscriptions:** base solution platform upfront cost, user licencing/subscription costs, add-on modules, storage and API costs.
- ↳ **Implementation services:** vendor/partner assisted system configuration, legacy system data migration, legacy system integrations, report/dashboard setup as well as several other system specific services that require technical assistance.
- ↳ **Hosting & infrastructure:** typically, Software as a Service (SaaS) or managed Platforms/Infrastructure as a Service (PaaS/IaaS – Cloud Services), billed monthly. If self-hosting (On-Premises) an open-source distribution will cost once off, additionally, decentralised solutions will attract a network connectivity cost. All endpoint devices if not available will be required for the initial system installation.
- ↳ **Support & maintenance:** vendor support plan, partner retainer for enhancements, minor releases, and specialised maintenance.
- ↳ **Capacity building:** training, onboarding materials, and (where needed) localisation (language and geographical specific considerations).

B.

Risks and Mitigation of off-the-shelf systems

All software carries risks, for off-the-shelf systems, the main exposures and mitigations are:

- ↳ **Vendor lock-in / roadmap dependence:** Mitigation is achieved via contractual **data-export rights** as well as defined and agreed exit clauses before conclusion of purchase agreements. Additionally, the use of open formats, and periodic market reviews is suggested.
- ↳ **Cost escalation (licences/add-ons):** *Mitigation is achieved* when agreeing on multi-year price caps, defined system usage forecasting, and approved system add-ons.
- ↳ **Data sovereignty constraints:** *Mitigation is achieved* by selecting in-country cloud hosting vendors, strong DPAs, and documented residency controls with the vendors (no outsourcing to other vendors).
- ↳ **API/automation limits & integration issues:** *Mitigation is achieved* with early capacity planning, API tier selection, and Enterprise Service Bus (ESB) integrations.
- ↳ **Over customisation (technical debt):** *Mitigation is achieved* with a **configuration-first policy**, design guardrails (pre-agreed constraints, standards, and defaults that steer solution design), and a change advisory board for all system changes.
- ↳ **Availability/system outage risk:** *Mitigation is achieved* via vendor **SLA** targets, tested backup/export procedures, and DR environments for mission critical systems.
- ↳ **Partner dependency / skills gap:** *Mitigation is achieved* by training internal administrators and retaining at least one alternate partner.

Strategic Benefits

- ↳ **Speed to value:** Solution/system deployment is fast; with a predictable project schedule - especially relevant when meeting donor milestones.
- ↳ **Proven workflows & compliance requirements:** Reduces delivery risks; leverages vendor certifications and audit trails.
- ↳ **Ecosystem & support:** Access to system partners, training, documentation, system interconnectors, and online marketplace add-ons (particularly relevant with open-source solutions/systems).
- ↳ **Scalability:** Capacity and features scale with institutional growth without having to re-engineer.

2.2 INTERNALLY DEVELOPED BESPOKE NHRI SYSTEM (OPEN SOURCE)

A.

What it requires

An internally developed solution assembles proven open-source components that when combined delivers solutions that meet NHRI requirements, mandates, and processes. Developing an open-source system involves using publicly available software components and platforms that can be freely modified and redistributed. Additionally, there are free resources available which technologists can make use of relatively cost effectively. While many costs within the open-source software stack are free, it does and can have associated costs attached to it, particularly if enterprise services within the open-source stack is required. To that end the following applies too internally designed and developed bespoke software:

Key Roles (Some of these roles may be fulfilled by the same individual)

- ↳ **Product Owner (business):** owns scope and priorities; signs off features against NHRI requirements.
- ↳ **Project/Delivery (Project Management Office):** plans delivery sprints, budget, vendors/partners, and delivery risks.
- ↳ **Business Process Analysis:** elicits requirements, defines workflows, forms, user stories, system acceptance criteria.
- ↳ **Solution/Systems architecture** designs the overall solution (auth, secure submissions, storage, RBAC, integrations).
- ↳ **Developers (open-source stack):** configure/adapt components; build NHRI-specific modules.
- ↳ **DevOps/Release Engineer:** manages environments (Dev/Test/Prod), continuous integration and continuous delivery, versioning, and deployments.
- ↳ **Testing & QA:** runs functional, user, and security tests; verifies the system meets stated requirements.

Technology

- ↳ **Open-source selection:** choose reliable, well-maintained components that match development and support needs.
- ↳ **Environments:** provide **Development, Test/Sandbox, and Production** (cloud or on-prem) to build, verify, and operate the system.
- ↳ **Foundations:** identity/SSO, secure evidence storage, role-based access (RBAC/UBAC), monitoring/logging, backups and restore procedures.

Processes

- ↳ **Training & documentation:** role-based curricula; user/admin manuals; onboarding and refresher plans.
- ↳ **ICT governance & best practice:** adopt frameworks for change/incident/problem management; secure SDLC/DevSecOps; standards for configuration, release, and support.
- ↳ **SOPs:** approved procedures for complaints, investigations, National Prevention Mechanism visits, UPR tracking, FOI timelines; QA checklists; change control.

Financial requirements for internally developed bespoke NHRI systems

Costing associated with the development of bespoke systems has a startup cost which is high and then levels out as the project progresses and then once the system is deployed it costs again. Maintenance and support will be the same as off-the-shelf systems.

- ↳ **Licensing costs:** open-source platforms generally have lower costs and, in some instances, eliminate the need for expensive software licenses. It is however to be noted that costs are associated with open-source platforms and that these need to be further explored.
- ↳ **Development costs:** these include hiring developers, user interface/user experience designers, project management, Business Analysts, Systems Architects as well as the technologists required to support the bespoke systems.
- ↳ **Hosting & infrastructure:** can be on-premises or cloud-based, depending on institutional strategy.
- ↳ **Support & maintenance:** while the codebase is free, technical support (internal or outsourced) is essential and will require budgeted funds.
- ↳ **Capacity building:** includes user training, onboarding materials, and potentially localized language support.

B.

Risks and Mitigation of inhouse developed bespoke systems

With all software regardless of off-the-shelf or in-house developed bespoke systems there are always risks associated with it. Below we will discuss the risks associated with bespoke systems that have been developed, modified and supported by an organization.

- ↳ **Sustainability risk:** without ongoing support and maintenance, the system may degrade over time. Mitigation is achieved by building local technical skills and capacity as well as establishing a clear maintenance plan with an associated technology roadmap.
- ↳ **Security vulnerabilities:** open-source platforms require vigilant ongoing monitoring for threats. Mitigation is achieved by implementing a robust maintenance schedule.
- ↳ **Skill gaps:** some NHRIs may lack in-house expertise. Mitigation is achieved by leveraging local tech ecosystems, universities, or regional partners to close the skills gap and build internal capacity.
- ↳ **Integration complexity:** combining new systems that have been developed with legacy systems, and their associated databases may be complex. Mitigation is achieved by making use of APIs and middleware components such as ESB's for seamless solution/system integration.

Strategic Benefits

There are certainly several benefits to developing one's own bespoke systems, however it requires a very mature and well-defined structure to achieve. Below are several additional strategic benefits that organizations can achieve with this model:

- ↳ **Scalability:** systems can evolve based on institutional needs without vendor lock-in. Additionally, the data collected remains the property of the organization with no vendors having a say in the data within the systems developed.

- ↳ **Adaptability:** bespoke systems allow for rapid customization, multilingual interfaces, and integration with global standards as is required within the digital strategy the country has chosen.
- ↳ **Cost Reduction:** open code bases, if managed correctly, tend to promote an environment of software efficiency directly impacting both Capital Expenditure and Operating Expenditure budgetary line items.

3. AI IN NHRI SYSTEMS

AI can significantly strengthen the work of NHRIs by supporting case management, data analysis, and public engagement.

Many AI-enabled capabilities build upon digital foundations outlined in earlier sections of this Toolkit, particularly structured case management systems and reliable data collection. Once these systems are in place, AI techniques such as machine learning and automated text analysis can help NHRIs extract greater value from their data.

For example, AI can help institutions in managing increasing volumes of complaints, by categorizing complaints (triage), flagging urgent cases, and identifying patterns in data that reveal systemic human rights violations. This allows NHRIs to respond more quickly and make evidence-based policy recommendations. AI tools such as chatbots or virtual assistants can provide accessible guidance to the public on their rights and complaint procedures, while automation of routine tasks like document classification and record keeping frees staff to focus on investigations and strategic work. It is important for NHRIs to ensure human oversight in AI systems to ensure that technology supports, rather than undermines human rights principles and address related risks.

EXAMPLES OF AI SOLUTIONS

Automation technologies can streamline internal administrative processes. AI-enabled document management systems can automatically classify and prioritize files, complaints, extract relevant information from uploaded evidence, and organize case records. Machine learning models can also support automated document summarization, allowing investigators and legal teams to review case materials more efficiently.

Machine learning techniques allow institutions to analyze large volumes of complaints, investigation records, and external datasets to identify patterns or emerging trends in human rights violations. For instance, AI models may detect geographic clusters of complaints, recurring violations by particular institutions, or correlations between policy changes and complaint volumes. These insights can strengthen evidence-based reporting and policy recommendations.

Natural language processing (NLP) allows systems to analyze and interpret large volumes of text-based data. Since many complaints are submitted in narrative form, NLP tools can help extract key information from written submissions, analyze testimonies, identify recurring themes, summarize case details, or translate submissions into multiple languages. This can improve accessibility while reducing the manual effort required to review and categorize complaints, reports, documentation of human rights violations.

Chatbots and virtual assistants can guide the public through complaint procedures, explain their rights, and provide information on available remedies. These tools can operate through websites, mobile applications, or messaging platforms, allowing NHRIs to provide assistance outside of normal office hours and reach individuals who may not be able to visit physical offices. AI-powered systems can also help triage initial inquiries, ensuring that staff time is focused on complex or sensitive cases.

Early warning systems: At a more advanced stage of digital maturity, NHRIs may explore **predictive analytics**. These systems analyze historical data to anticipate potential trends in complaints or identify risk indicators for emerging human rights concerns. While predictive models should never be used as sole decision-making tools, they can help institutions allocate resources more effectively and support proactive monitoring of systemic issues.

Key considerations for responsible AI use include:

While AI offers significant opportunities, its implementation in NHRIs requires careful consideration to ensure that technology supports, rather than undermines human rights principles.

↳ **Data quality and governance**

AI systems require accurate, complete, and validated data to function effectively. NHRIs must ensure that their case management systems maintain accurate and validated data, supported by clear data governance frameworks.

↳ **Ethics and bias mitigation**

AI systems may inadvertently replicate biases present in data or training models. AI systems must therefore not replace human decision making to avoid possible system discrimination.

↳ **Transparency and human oversight**

NHRIs should maintain transparency about how AI tools are used within their systems. Where possible, institutions should prioritize AI models that provide explainable outputs so that decisions supported by AI can be clearly understood and justified.

↳ **Human oversight and accountability**

AI systems should support decision-making rather than replace human judgment. Investigations, legal determinations, and findings of human rights violations must remain under the authority of qualified NHRI staff.

↳ **Privacy and data protection**

Human rights complaints often involve sensitive personal information. NHRIs should ensure that the chosen AI systems operate within national data protection laws and institutional privacy policies, confirming secure data handling and responsible use.

Challenges in implementation of AI components may include limited technical capacity, high infrastructure costs, and gaps in legal or regulatory frameworks. Public trust is also essential; populations need confidence that AI is used responsibly and that their personal data will be handled securely. Transparency in how AI tools are used, as well as clear safeguards and human oversight are essential for maintaining this trust.

For most NHRIs, the adoption of AI should follow a gradual and carefully managed approach. **Best practices** suggest starting with pilot projects such as automated complaint classification or chatbot-based guidance, then integrating AI gradually and always engaging with stakeholders. Additionally, it is recommended that organizations conduct regular audits to ensure accuracy, fair-

ness, and compliance are ongoing. When implemented thoughtfully, AI can enhance operational efficiency, strengthen NHRI decision-making, and improve accessibility for the public.

4. ALIGNING SOLUTIONS WITH NATIONAL DIGITAL INITIATIVES

It is crucial for institutions to align their digital strategies with national digital initiatives in their country to ensure interoperability, legal compliance, and the effective implementation of digital services. Furthermore, most countries have invested in the Digital Public Goods 7 domain and it's therefore important that an alignment to these initiatives takes place as it secures system sustainability.

Institutions should:

- ↳ Regularly review their country's digital strategy documents to understand key priorities, goals as well as policy adaptations.
- ↳ Ensure that their internal digital policies and frameworks align with data protection and hosting rules.
- ↳ Engage with national regulatory bodies and digital agencies to stay informed about emerging trends, standards, and best practices and finally
- ↳ Foster collaboration with public and private sector stakeholders to enhance digital transformation efforts.

5. CONCLUSION AND NEXT STEPS

Completing the Digital Pre-requisites screening and the Digital Readiness Self-Assessment Checklist represents an important milestone for NHRIs. This Toolkit is designed to help NHRIs assess their current digital capacities, identify strengths, and highlight areas where further development may be required. By providing a structured overview of institutional practices across key dimensions of digital readiness, the assessment enables NHRIs to gain a clearer understanding of where they stand in their digital transformation journey.

The results of the Digital Readiness Assessment should be viewed as a starting point for strategic planning rather than an endpoint. Once an NHRI has completed the Checklist and determined its maturity level, the next step is to translate these insights into a practical and achievable action plan. This process allows institutions to move from assessment to implementation in a structured and sustainable manner. Where available, findings from the NHRI Capacity Assessment may also be used alongside the results of the Digital Readiness Assessment to support integrated institutional planning. The Digital Readiness Toolkit can also inform the capacity assessment process. This is increasingly important, as more NHRIs adopt and rely on digital systems.

As a first step, NHRIs may wish to review and validate the findings from the digital readiness assessment internally. This can involve consultations with relevant units within the institution, such as leadership, information technology teams, complaints handling units, and monitoring or research departments, to ensure a shared understanding of the results and to confirm priority areas for improvement.

Based on this internal reflection, the institution can then develop a Digital Readiness Action Plan that outlines concrete steps to strengthen its digital systems and practices. Depending on the NHRI's maturity level, this plan may be structured across different time horizons. For example,

- ↳ *Short-term actions* may focus on foundational improvements that can be implemented relatively quickly. These could include strengthening basic cybersecurity practices, improving internal policies on data protection and information management, conducting staff awareness and training sessions, or addressing critical gaps in digital tools and procedures.
- ↳ *Medium-term actions* may involve more structured institutional improvements. These might include upgrading digital infrastructure, improving case management or complaint intake systems, developing secure digital platforms for communication and reporting, or strengthening internal governance and coordination mechanisms for digital initiatives.
- ↳ *Long-term actions* may focus on strategic transformation and sustainability. This could include the development of integrated digital systems, advanced data analysis capabilities to support human rights monitoring, stronger digital engagement with the public, and the integration of digital innovation into broader institutional strategies and planning processes.

Throughout this process, NHRIs are encouraged to adopt a phased and realistic approach that reflects their institutional context, available resources, and national environment. Digital transformation does not require immediate large-scale investments; rather, it is often most effective when built gradually through targeted improvements and continuous learning. Engaging with partners and peers can also play a valuable role. NHRIs may benefit from sharing experiences with other institutions, seeking technical support where needed, and drawing on existing resources and guidance provided by partners.

Ultimately, digital transformation should serve one purpose above all others; strengthening the ability of NHRIs to protect and promote human rights for all. This Toolkit therefore encourages institutions to move forward in a deliberate and measured manner starting with self-assessment, building internal capacity, managing risks proactively and continuously reviewing impact, so that digital systems become trusted enablers of independence, integrity and effectiveness, rather than sources of new vulnerability. Through sustained leadership, sound governance and people-centred design, NHRIs can build digital foundations that support both present operational needs and future institutional resilience.

By taking these next steps, NHRIs can build on the insights gained from the digital readiness assessment and move toward stronger, safer, and more effective digital systems that enhance their ability to promote and protect human rights in an increasingly digital world.

ANNEX 1



Technical components to consider

The section below provides a quick reference guide to various technology Infrastructure components that would need to be considered when looking at NHRI digital transformation.

1. DIGITAL TECHNOLOGY (CLOUD VS ON PREMISES)

COMPONENT	ATTRIBUTE	CLOUD-BASED SOLUTION	ON-PREMISES SOLUTION
INFRASTRUCTURE (Servers)	Definition	Remote virtual servers hosted by providers such as Amazon Web Services (EC2), Microsoft Azure (Virtual Machines), or Google Cloud Platform.	Involves physical servers from vendors like HP, Dell, or IBM deployed in local data centers.
	Security & Compliance	High-level security with built-in compliance options (ISO, GDPR, etc.), however an institution relies on third-party service providers to ensure services are secure.	Institutions have full control over their own security however it requires constant updates and monitoring internally to an institution.
	Data Control & Privacy	Data is stored externally, raising concerns over data sovereignty particularly citizen data.	Full control over data storage and access policies as data storage is done inhouse.
	Compliance with Local Laws	May require specific regional cloud providers for compliance.	Easier to align with local regulatory requirements, particularly data specific laws.
	Setup & Deployment	Quick setup with minimal hardware needs.	Requires procurement, setup, and configuration of hardware as well as ongoing maintenance.
	Scalability	Highly scalable, the solution allows for both an increase and decrease in physical resources as is needed.	Limited by existing hardware that is available, requiring additional investment for system expansion.
	Maintenance	Managed by cloud service providers, including system updates and security components.	Requires in-house IT team for maintenance and updates.
	Cost	Subscription-based pricing (Operating Expenditure); lower upfront costs but recurring expenses.	High upfront Capital Expenditure; lower ongoing costs but higher maintenance.
	Note	NOTE: Some governments set up their own centralized cloud services for a negotiated fee.	Performance scaling is hardware-bound and typically slower than cloud environments.

SOFTWARE (Applications & OS)	Maintenance	Managed by cloud service providers, including system updates, patching, and security components.	Requires in-house IT team for manual updates, patches, and version control.
	Customization	Limited customization due to service provider restrictions and standardized environments.	Full control over bespoke software and hardware customization to meet specific organizational needs.
	Accessibility	Easily accessible from anywhere with internet connectivity; ideal for agile, remote access.	Limited remote access; requires VPN or special configurations managed by a dedicated technical team.
	Compliance	May require specific regional cloud providers for compliance with local data sovereignty laws.	Easier to align with local regulatory requirements and data-specific laws.
NETWORKS (Connectivity)	Security & Architecture	Service providers provide secure access points, enterprise-grade routers, VPN concentrators, and firewalls.	Requires full ownership of the internal network infrastructure, including routers, managed switches, firewall appliances and VPN services.
	Remote Accessibility	Easily accessible from anywhere with internet connectivity.	Limited remote access requires VPN or special configurations managed by a dedicated technical team.
	Performance	Dependent on internet connection, potential latency issues are characteristically issues that one needs to contend with.	Generally faster within a private network but requires redundancy planning when networks face challenges.
DATA PROTECTION (Backups/DR)	Disaster Recovery	Automated backups and disaster recovery options included.	Requires a dedicated disaster recovery setup and backup planning (Network-Attached Storage, redundant array of independent disks, etc.).
	Managed Services	Paid services ensure automated backups, version control, and off-site redundancy, ensuring high availability at a monthly cost.	Manual oversight or third-party software is often needed to schedule and monitor backups.

2. ICT BEST PRACTICES (GOVERNANCE, SUSTAINABILITY AND DELIVERY)

Effective ICT maintenance and governance are essential components of institutional resilience and accountability. As digital systems start underpinning core operational functions i.e. case management, communications, data storage, analytics and data reporting, it is critical to ensure their reliability, business continuity, security, and alignment with institutional mandates. It's therefore important that regardless of the actual systems implemented, core foundational ICT governance, frameworks and best practices should be considered as part of the overall ICT landscape in the organization.

2.1. ICT MAINTENANCE

Effective and efficient ICT maintenance¹⁸ goes beyond routine system fixes and patches, it ensures digital business continuity, a reduction in system risks, and the preservation of institutional credibility. Maintenance of digital services and systems encompasses four key categories which are listed below:

- ↳ **Preventive Maintenance:** This is comprised of scheduled hardware diagnostics checks, software patching, and overall system updates in order to not only ensure ongoing system performance and availability but to be in a position to pre-empt possible system failures.
- ↳ **Corrective Maintenance:** Requires the ability to rapidly response to system faults or security breaches, minimizing operational downtime and ensuring business continuity.
- ↳ **Adaptive Maintenance:** Modifying systems in response to policy changes, evolving needs, or compliance and regulatory needs.
- ↳ **Perfective Maintenance:** Ongoing and continuous improvements which effect performance positively, usability, and user experience.

ICT maintenance and governance are no longer back-office functions, they are strategic enablers of institutional performance, accountability, and resilience. Through deliberate planning, international best practice, and sustained investment in human and digital capital, NHRIs can ensure their digital infrastructure is secure, compliant, and fit for the future.

EXAMPLE

Estonia's digital governance infrastructure is lauded globally due to its rigorous preventive and adaptive maintenance of its national e-government platform (e-Estonia)¹⁹. Additionally, 100% of their government services are digital.

¹⁸ <https://www.itil.com/>

¹⁹ <https://e-estonia.com/>

2.2. ICT GOVERNANCE AND FRAMEWORKS

ICT governance, however, ensures that technology investments and operations support the institution's strategic goals. Governance frameworks should be based on internationally recognized standards, such as:



Governance:

COBIT (Control Objectives for Information and Related Technologies)²⁰: Offers a model for aligning IT goals with business objectives.

ISO/IEC 38500²¹ Provides principles for effective corporate governance of IT.



Service management

ITIL (Information Technology Infrastructure Library)²²: Is a globally recognised framework for IT Service Management (ITSM) that provides best practices for delivering high-quality IT services aligned with business needs. Developed originally by the **UK Government's Central Computer and Telecommunications Agency** in the 1980s, ITIL has evolved through several versions and is now managed by **AXELOS**.



Architecture & integration

SOA (Service Orientated Architecture)²³ Is a software design paradigm that structures applications as a collection of loosely coupled, interoperable services. Each service represents a discrete unit of functionality – such as user authentication, data retrieval, or case tracking – that can be reused and combined to support different business processes within an organization.



TOGAF²⁴ Stands for The Open Group Architecture Framework. It is a proven enterprise architecture methodology and framework used to design, plan, implement, and govern an organization's enterprise information architecture. Developed by The Open Group, TOGAF provides a structured approach for aligning IT systems with business goals, helping organizations manage complexity, reduce risk, and support long-term strategic planning.

NOTE

Various ICT Governance and Service Management Resource template links can be found in the NHRI Toolkit Companion Resources Repository ([Annex 2](#))

20 <https://www.isaca.org/>

21 <https://www.iso.org/>

22 <https://www.itil.com/>

23 <https://www.opengroup.org/what-we-do-technology-standards/soa/source-book/intro>

24 <https://www.opengroup.org/togaf>

3. IMPORTANT KEY ICT PRINCIPLES

- ↳ **Accountability:** A well-defined ICT departmental organogram must be developed and in place, defining roles and responsibilities which is clearly assigned to avoid ambiguity internally to the organization.
- ↳ **Transparency:** A well-defined and document ICT policies must be developed and in place as this component is essential in achieving a mature digital status.
- ↳ **Compliance:** Adherence to data protection and cybersecurity regulations (e.g., POPIA in South Africa or GDPR in Europe) is vitally important particularly when it effects human rights issues.
- ↳ **Risk Management:** Ongoing assessments of cyber risks, vendor reliability, and technological obsolescence is important and must be part of an ICT 5-year road map.

4. DIGITAL SUSTAINABILITY AND CAPACITY BUILDING

A well-maintained and governed ICT ecosystem includes institutional mechanisms for sustainability. The four key points below provide a list of 'must haves', particularly when one is considering the implementation of highly mature digital ICT systems. For an organization to maintain mature ICT systems, the ICT department must be well staffed and managed, with defined processes in place.

- ↳ **Training and Skills Development:** Continuous professional development in cybersecurity, data governance & management, as well as internal ICT systems.
- ↳ **ICT Policy Frameworks:** Internal ICT policies to guide usage, access control, procurement, and incident response.
- ↳ **Monitoring and Evaluation:** Use of Key Performance Indicators, system audits, and usage analytics to assess ICT performance and value.

Public-Private Collaboration: Partnering with academic, tech, and civil society actors for innovation, cost-efficiency, and skills transfer.

EXAMPLE

Rwanda's Irempo platform, designed to deliver e-government services, combines in-house development with external partners and emphasizes training for local ICT staff.

5. RECOMMENDATIONS FOR IMPLEMENTATION OF DIGITAL SERVICES IN NHRIS

Establish an ICT Governance Board reporting to senior leadership.

- ↳ Adopt open standards and frameworks like ISO/IEC 27001 and COBIT 2019.
- ↳ Allocate dedicated budgets for ICT maintenance, upgrades, and staff development.
- ↳ Leverage cloud-based monitoring tools for predictive maintenance.
- ↳ Create cross-functional ICT risk registers to document and monitor threats.

6. ICT PROJECT MANAGEMENT FOR NHRI DIGITALIZATION

To achieve and deliver on a digital transformation program within any organization or institution a structured project management methodology must be adopted. It ensures successful planning, implementation, and long-term sustainability of a system and service regardless of the institution or organization it is servicing. ICT project management provides the tools and methodologies that are necessary to manage risks, defined timelines, and budgets while at the same time aligning system development with institutional requirements and stakeholder needs.

In the context of NHRI's, project management will need to accommodate complex governance components, evolving mandates, and varied stakeholder interests. Whether one is applying Agile²⁵, Waterfall²⁶, Prince II²⁷, or a hybrid, a well-governed project will ensure the following:

- ↳ Clearer scope definition with a well-defined phased approach.
- ↳ Ensure active stakeholder engagement, including legal, administrative, and technical teams (implementing or development teams).
- ↳ Ensure monitoring and evaluation mechanisms throughout the project lifecycle and
- ↳ Assist with capacity-building for internal teams to reduce vendor dependency over time the medium to long term.

Embedding project management practices into a NHRI digitization effort helps institutions avoid common pitfalls such as scope creep, cost overruns, and delays, while fostering a culture of accountability and continuous service improvement not to mention transparency.

NOTE

Various Project, Design, and Assessment Resources template links can be found in the NHRI Toolkit Companion Resources Repository ([Annex 2](#)).

7. ESSENTIAL TEMPLATES AND POLICIES

To ensure digital systems meet both user expectations and institutional mandates, it is critical to define and document system needs clearly through BRS and Functional Requirement Specifications (FRS). These two documents serve as the foundation for system procurement, development, and implementation, whether an organization is investing in off-the-shelf platforms or developing bespoke in-house solutions adhering to globally excepted ICT framework is critical.

25 <https://www.openproject.org/>

26 <https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model>

27 <https://www.openproject.org/blog/prince2-with-openproject/>

7.1. REQUIREMENT TEMPLATES

BRS outlines the high-level goals, stakeholders, and operational outcomes expected from the system. It serves as a blueprint for aligning the digital tool set with NHRI mandates, workflows, and intended outputs.

↳ **FRS** translates those goals into detailed functional expectations and system behavior, including user interactions, input/output processes, integration points, and compliance features.

These templates ensure consistency, transparency, and accountability in how systems are planned and deployed. The documents also include key considerations for choosing between custom-developed versus off-the-shelf systems, considering cost, capacity, localization needs, and long-term maintenance.

NOTE

BRS & FRS Document templates can be found in the Project Management folder.

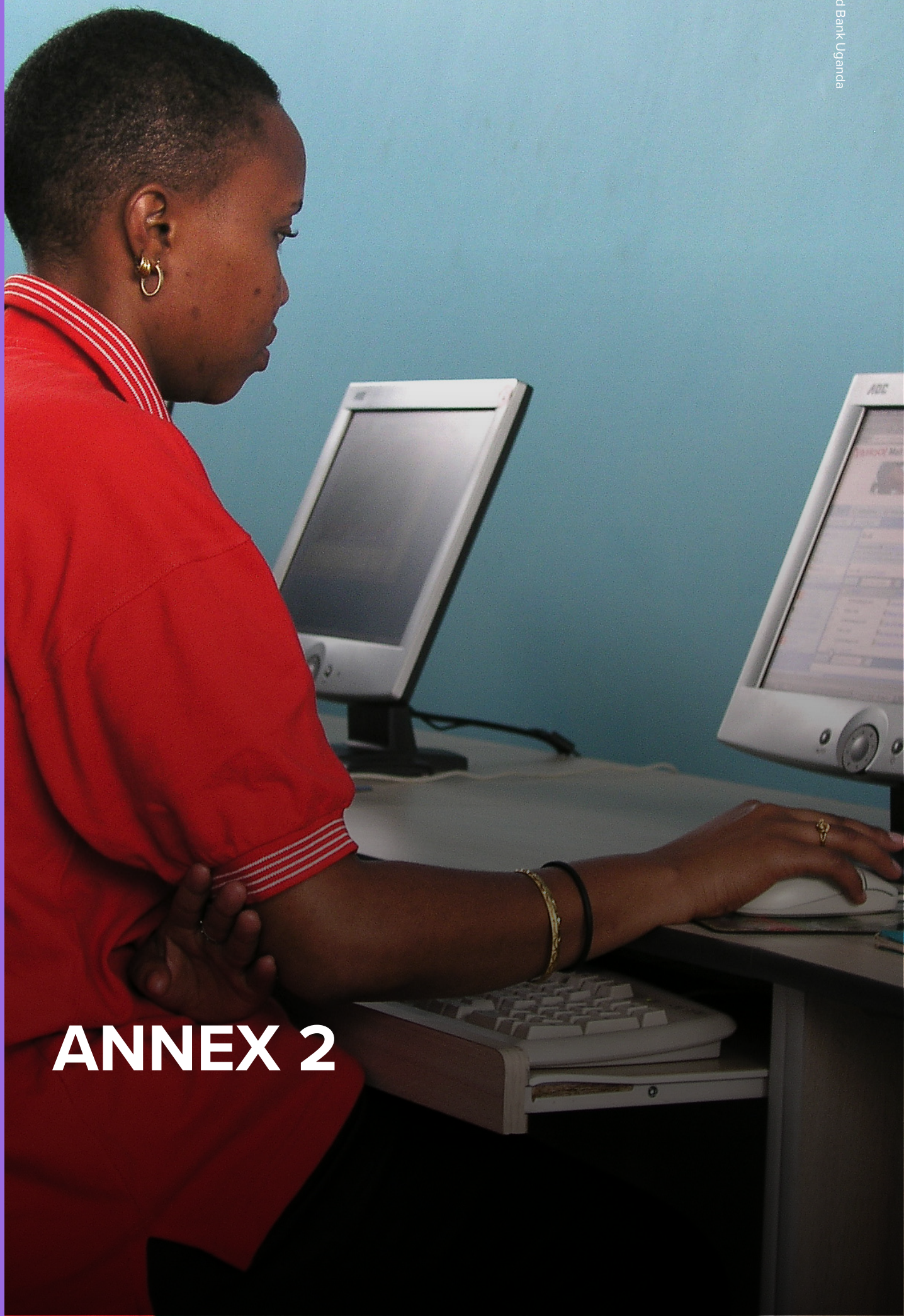
7.2. CORE ICT POLICIES FOR NHRIS

Achieving a higher digital maturity request that robust ICT policies are implemented as part of the overall ICT strategy as it is essential to ethical, secure, and efficient use of digital systems. These policies ensure that digital tools and data are managed in compliance with national regulations, international standards, and institutional mandates.

Key ICT policies that NHRIs should consider include:

- ↳ **Usage Policy** – The policy that outlines the guidelines which define the proper use of institutional devices, networks, and data.
- ↳ **Data Protection and Privacy Policy** – Defines how personal and sensitive data is collected, processed, stored, and shared in accordance with national laws.
- ↳ **Information Security Policy** – Covers cybersecurity standards, encryption protocols, access control measures (RBAC), as well as incident response procedures.
- ↳ **Backup and Disaster Recovery Policy** – Ensures business continuity (stated within ITIL) of operations through data redundancy, offsite/cloud backups, and recovery strategies (Mean Time to Repair, Recovery time objectives etc).
- ↳ **Software Procurement and Licensing Policy** – Establishes protocols for acquiring and managing software licenses within the legal mandate cost effectively.
- ↳ **ICT Governance and Change Management Policy** – Guides decision-making on system upgrades, user feedback, and alignment with organizational strategy.

ANNEX 2



1. NHRI TOOLKIT COMPANION RESOURCES REPOSITORY

Public reference links and companion resources for use alongside the NHRI Digital Readiness Toolkit

Purpose: This repository is designed to accompany the NHRI Digital Readiness Toolkit by pointing users to public templates, guidance, and reference materials that can help institutions develop their own governance, service management, project design, and digital planning documents. Where an exact public equivalent was not identified, the closest practical public reference has been listed. The Digital Maturity Self-Assessment is referenced as an appendix to the toolkit.

NOTE

“Primary public reference” points to the most useful publicly available starting point; “Supplementary reference” points to an additional guide, framework, or example that can strengthen adaptation for NHRI use.

1.1 ICT GOVERNANCE AND SERVICE MANAGEMENT RESOURCES

NHRI COMPANION RESOURCE	PUBLIC REFERENCE	PURPOSE / HOW IT SUPPORTS THE TOOLKIT	ACCESS	NOTES
Digital Technology Policies – NHRI Framework	NCSC Cyber Security Toolkit for Boards UK Blueprint for Modern Digital Government	Provides governance framing for digital policy, oversight, cyber risk, leadership accountability, and longer-term digital planning.	Public web link	No single public NHRI-specific equivalent identified; combine governance and digital strategy references when adapting.
NHRI ICT Policies & Procedures	Data Protection Policy Template Sample Government IT / Email / Computer Policy	Useful starting points for acceptable use, privacy, staff responsibilities, and broader ICT policy drafting.	Public web link	These are generic public examples and should be adapted to NHRI legal, privacy, and governance requirements.

NHRI Service Desk Description	How to Build a Service Desk IT Service Management Template Overview	Supports the design of a basic service desk, request routing, support workflows, and user-facing support channels.	Public web link	Useful for institutions building first-line ICT support and service request handling.
NHRI Incident Management	Incident Management Template CISA Cybersecurity Incident & Vulnerability Response Playbooks	Provides practical references for incident logging, response roles, escalation, communication, recovery, and post-incident learning.	Public web link	The CISA playbooks are more advanced but useful for building structured incident response arrangements.
NHRI Problem Management	Problem Management Template Problem Management Process Overview	Helps institutions move from resolving individual incidents to identifying root causes and preventing recurrence.	Public web link	Best used after basic incident management is already defined.
NHRI Change Management	Change Management Plan Guide and Template IT Change Management Overview	Supports the controlled approval, implementation, and review of changes to systems, services, and digital processes.	Public web link	Suitable for both organisational change and ICT/system change control.
NHRI Release Management	Product Release Guide Release Planning Page Guide	Provides reference approaches for planning, coordinating, documenting, and communicating releases or system updates.	Public web link	Public guidance is more product/software oriented; adapt to institutional system releases and controlled deployments.
NHRI 5-Year Roadmap Template	Project Roadmap Templates Change Roadmap Templates	Supports the preparation of phased digital roadmaps, milestones, sequencing, and long-term planning.	Public web link	Useful as a practical planning companion to the toolkit pathways and maturity model.
ITIL Presentation	ITSM Overview NCSC Cyber Governance for Boards	Provides accessible introductory material on service management, governance, and the role of structured ICT practices.	Public web link	Useful for orientation, training, and awareness raising rather than as a formal template.

1.2 PROJECT, DESIGN, AND ASSESSMENT RESOURCES

NHRI COMPANION RESOURCE	CLOSEST PUBLIC REFERENCE	PURPOSE / HOW IT SUPPORTS THE TOOLKIT	ACCESS	NOTES
ICT Project Methodology	Agile Project Management Templates Project Management Templates Library	Supports project initiation, planning, execution, iteration, governance, and delivery management for digital initiatives.	Public web link	Can be used to build a light project methodology for ICT and digital transformation work.
NHRI Business Specifications Document	Business Requirements Document Templates	Helps institutions define business needs, scope, stakeholders, objectives, assumptions, and expected outcomes before solution design.	Public web link	A practical starting point for drafting BRS/BRD-style documents.
NHRI Functional Requirements Specification Document	Functional Specification Templates Project Requirements Templates	Supports the definition of functional requirements, expected system behaviour, workflows, and detailed solution requirements.	Public web link	Useful once the business case and business requirements have already been clarified.
NHRI Internal Digital Self-Assessment Document	Data Maturity Assessment for Government: Framework	Supports institutional self-reflection on digital maturity, readiness, and priority areas for improvement.	Public web link	The NHRI Digital Maturity Self-Assessment should be included as an appendix to the toolkit; the GOV.UK resource can be cited as a supplementary public reference.
Sample Business Specifications Document	Sample Business Requirements Document Template	Provides a worked example or starting structure that institutions can adapt when preparing their own business specification documents.	Public web link	Use together with the main business requirements template and the ICT project methodology reference.

