Gender Action Plan (GAP)

Digital Economy Enhancement Project

(DEEP)

April 2026

Table of Contents

List of Tables

Abbreviations

Abbreviation	**Acronym**
BoI	Board of Investment
CoC	Code of Conduct
CITL	Civic Innovation Technology Lab
CSOs	Community Service Organizations
CSP	Citizen Service Portal
DEEP	Digital Economy Enhancement Project
E&S	Environmental and Social
ESCP	Environmental and Social Commitment Plan
FGDs	Focus Group Discussions
GAP	Gender Action Plan
GBV	Gender Based Violence
GRC	Grievance Redress Committee
GRM	Grievance Redress Mechanism
H&GRCs	Harassment & Grievance Redress Committees
HGS	Health/Gender/Safety
ICT	Information and Communication Technologies
IEC	Information, Education and Communication
M&E	Monitoring and Evaluation
MoHR	Ministry of Human Rights
MoITT	Ministry of Information Technology and Telecommunication
MoUs	Memorandum of Understandings
NADRA	National Database and Registration Authority
NCCIA	National Cybercrime Investigation Authority
NCHR	National Commission for Human Rights
NCRC	National Commission on the Right of Children
NCSW	National Commission on Status of Women
NDEL	National Data Exchange Layer
NITB	National Information Technology Board
OTP	One-Time Password
PBP	Pakistan Business Portal
PC	Procurement Committees
PD	Project Director
PIEs	Project Implementation Entities
PIU	Project Implementation Unit
PMU	Project Management Unit
RoW	Right of Way
PSC	Project Steering Committee
RLCOs	Registration, Licenses, Certification and others
SEA/SH	Sexual Exploitation and Abuse/Sexual Harassment
SMEs	Small and Medium Enterprises
SOPs	Standard Operating Procedures
TORs	Terms of References
UX/UI	User Experience/User Interface
WB	World Bank
WBG	World Bank Group

1. Introduction: Context and Rationale

The Digital Economy Enhancement Project (DEEP), led by the Ministry of Information Technology and Telecommunication (MoITT) in collaboration with the World Bank (World Bank Funded Project), is a transformative project aimed at modernizing Pakistan's public service delivery, strengthening digital governance structure, and fostering inclusive digital economic growth. DEEP encompasses the development of critical digital public infrastructure (DPI) and citizen-centric platforms, including the National Data Exchange Layer (NDEL), National Citizen Service Portal (CSP), Pakistan Business Portal (PBP), Digital Innovation Hub, Civic Innovation Lab, Seed Grants and Open Data Portals, executed through NADRA, Citizen Services Team (NITB), BoI, and Civic Innovation Team (Ignite). These platforms collectively aim to facilitate secure, interoperable, and efficient interactions between citizens, businesses, and government institutions through easily accessible digital interfaces.

However, the systemic development of digital infrastructure is not intrinsically gender-neutral. Without intentional design and operational safeguards, digital transformation risks exacerbating existing gender inequalities and social vulnerabilities at all level. In Pakistan, women and marginalized populations often face intersecting barriers, such as, restrictive social norms, limited mobility, low digital and financial literacy, inadequate access to devices and connectivity, and obstacles in obtaining formal identification, which can prevent equitable participation in the development and utilization of Digital Public Infrastructure (DPI)/Platforms. These challenges are further intensified for rural women, persons with disabilities (PWDs), and other vulnerable groups.

In addition, the rapid expansion of digital services introduces new gender-differentiated risks, including online harassment, cyberbullying, digital fraud, identity theft, doxing, and misuse of personal data. Power asymmetries in in-person project engagements - including trainings, outreach, community facilitation, coordination, and civic innovation activities- can increase the risk of sexual exploitation, abuse, and harassment (SEA/SH) and technology-facilitated gender-based violence (TFGBV) against women and other marginalized participants if institutional safeguards are weak or inconsistently applied. These risks underscore the necessity of survivor-centered grievance mechanisms, anonymous reporting channels, secure data protocols (data protection rules), and gender-responsive interfaces.

This Gender Action Plan (GAP) has been developed in line with Pakistan's gender-related legislation, the World Bank Environmental and Social Framework (ESF), and Good Practice Notes on TFGBV, SEA/SH. The GAP systematically identifies gender-specific risks and prescribes mitigation measures across DEEP's digital ecosystem, more focusing on digital ID systems, citizen vaults/wallets, CSP, PBP, civic innovation labs, seed grants, open data portals, and NDEL interoperability frameworks. By embedding inclusive design, robust digital privacy and data protection protocols/rules, and safe complaint-handling mechanisms, this Action Plan aims to ensure gender equity, digital inclusion, and protection against online harassment, cyber threats, TFGBV and SEA/SH across all project activities. Continuous monitoring, ethical digital practices, and institutional accountability will be integral to maintaining a safe, accessible, and equitable digital public infrastructure for all users.

1.1. GENDER RISK FROM DIGITAL PUBLIC INFRASTRUCTURE (DPI): ACCESS AND SERVICE DELIVERY

Digital Public Infrastructure (DPI) including Digital Identity (ID) systems, Digital Vault/Wallet National Data Exchange Layers (NDEL) , the Citizen Service Portal (CSP), Pakistan Business Portal (PBP), Open Data Portal, Competitions, Seed Grants and Civic Innovation & Technology Labs (CITLs) - introduces gender-differentiated risks related to non-inclusive design and operation of digital infrastructures. Women, girls, and gender-diverse persons in Pakistan face deep-rooted structural barriers such as social restrictions on device use, limited mobility, lower digital and financial literacy, and reduced access to formal identification or SIM ownership. These inequalities heighten risks of exclusion from DPI-enabled services and increase vulnerability to unintended access and visibility of personal data, impersonation, misuse of identity credentials, and biased automated decision-making. Without gender-sensitive authentication process, privacy-enhancing features in design, and informed consent protocols for service accessibility, DPI can inadvertently reinforce gaps in access, agency, and safe participation across digital services in Pakistan.

The expansion of DPI into open innovation ecosystems, through platforms such as the digital vault/wallet, NDEL, CSP, PBP, open data portals and CITLs - creates additional exposure to digital harassment, cyberbullying, digital surveillance, identity theft, doxing, and digital or financial fraud. Women entrepreneurs, young female innovators, marginalized groups and other vulnerable groups participating in these digital spaces are particularly at higher risk due to limited protection of confidentiality, weak moderation systems, and male-dominated technical environments. Absence of survivor-centered complaint channels, anonymous reporting options, female-staffed support desks at all level of facilitation, and secure evidence-handling protocols/procedures, users may be discouraged from seeking help or reporting technology-facilitated abuse. DPI that does not embed gender-responsive safeguards measures, strong data protection rules, and inclusive governance of digital platforms can unintentionally magnify vulnerabilities and create unsafe participation environments across government, business, citizens and civic innovation platforms.

1.2. ONLINE HARRASEMENT AND CYBER (DIGTIAL) RISKS

The strengthened digital harassment and cyber-risk prevention framework under DEEP represents a structural shift from fragmented, institution-specific reporting arrangements toward a coherent, survivor-centered, and nationally coordinated digital complaint system.

By consolidating the reporting of online harassment, cyberbullying, blackmail, impersonation, digital fraud, doxing, data misuse, TFGBV, and SEA/SH into a unified digital grievance redress architecture, DEEP enables users to submit complaints through dedicated GRM interfaces embedded separately within the Citizen Services Portal (CSP) and the Pakistan Business Portal (PBP) (for business- and RLCO-related cases). Each portal operates its own secure, purpose-built complaint plug-ins, clearly distinguishing routine technical or service-related grievances from sensitive digital harm complaints. Sensitive cases submitted through CSP and PBP are automatically processed and routed via encrypted, rule-based plug-ins to the legally mandated competent authorities, without any manual handling, intermediary access, or discretionary intervention - ensuring confidentiality, consistency, and survivor safety.

Sensitive complaints are transmitted through automated routing mechanisms that direct cases to the appropriate authority based on complaint type and jurisdiction. Defined service-level timelines, tamper-proof audit trails, and system-generated accountability controls strengthen predictability, reduce delays, and enhance transparency across federal and provincial response institutions, while strictly preserving survivor anonymity and data integrity.

DEEP embeds survivor-sensitive and privacy-preserving design features across all relevant Digital Public Infrastructure (DPI), including anonymous and survivor-controlled reporting options, availability of trained female intake and triage support (where operationally feasible), encrypted evidence submission, masked identifiers, and strict role-based access to complaint data. These measures directly address persistent structural barriers: Such as fear of retaliation, loss of privacy, shared-device use, mediated access, and mistrust of institutions - that disproportionately prevent women, transgender persons, persons with disabilities, and other marginalized groups from seeking digital assistance. The framework prioritizes informed consent, non-retaliation, data minimization, and trauma-informed engagement, consistent with international best practices on TFGBV, SEA/SH, and cyber harassment prevention.

Beyond response mechanisms, DEEP adopts a preventive digital safety approach through in-portal cyber-safety guidance, consent-based data-sharing controls, secure access and recovery features, and targeted awareness and outreach initiatives. Aggregated, non-identifiable learning from complaint trends, system performance, and platform usage feeds into continuous system improvements, policy refinement, and adaptive safeguards - without compromising survivor confidentiality or system integrity.

Through this integrated model, DEEP establishes a holistic digital safeguards ecosystem that mitigates gendered digital risks while enabling women, youth, entrepreneurs, and vulnerable groups to participate safely and confidently in Pakistan’s digital economy. The framework ensures that digital transformation under DEEP does not inadvertently reinforce existing inequalities, but instead advances trust, inclusion, accountability, and safety across all digital platforms and engagement modalities supported by the project.

2. Project Overview/Summary of Project[1]

DEEP will support activities that will increase access to and promote the use of digital services across Pakistan. The Project Development Objective (PDO) is to enhance the Government's capacity for digitally enabled public services delivery for citizens and businesses.

The project will also support cross-cutting improvements in the enabling environment-supporting reforms to expand broadband connectivity and to strengthen the policy and legal framework for the digital economy. DEEP will also enable institutional, policy, and regulatory global best practices through technical assistance to the management and implementation agencies - including the MoITT, NADRA, Citizen Services - National IT Board (NITB), Board of Investment (BoI) and Civic Innovation - Ignite. Under the project, NADRA (National Database & Registration Authority under the Ministry of Interior) will build a data exchange layer for government agencies to exchange information securely, as well as provide citizens with a digital 'vault' to secure credentials. This is potentially transformative for increasing citizens' access to public and private services (everything from birth certificates to banking).

The proposed outcome indicators for the Project are as follows:

1. Transactions on the National Data Exchange Layer (Number)
2. Unique users on the National Citizen Services Portal (of which are female initiated) (Number and percentage)
3. Registration, Licenses, Certificates and Other (RLCOs) transaction processed on the Pakistan Business Portal (of which processed for female-led small and medium enterprises) (Number and percentage)
4. Users satisfied with services offered by the National Citizen Services Portal (Number and Percentage)

2.1. PROGRAM DESCRIPTION

Component 1: Improving digital economy, governance and service capabilities. This component will provide technical assistance to the Ministry of Information Technology and Telecommunications (MoITT) for policy and regulatory reforms to address regulatory and market failures in the country's connectivity infrastructure. It will include:

i. Right-of-Way (RoW) reforms, development, and adoption of a RoW-single-window, onboarding and change management of major civic agencies in the RoW-single-window, and development of RoW dispute resolution procedures.

[1] Stakeholder Engagement Plan (SEP of Digital Economy Enhancement Project (DEEP): https://documents1.worldbank.org/curated/en/099061823075042932/pdf/P1744020fd9a5f0d0be720a4b4da3eed09.pdf

ii. Broadband demand analysis and stimulation options to improve the affordability of smartphones and update of digital services.
iii. Broadband infrastructure mapping, assessment of market failures.
iv. Review and recommendations on the institutional and structural alignment of MoITT to meet emerging challenges and opportunities for digital transformation.
v. Nationwide stakeholder engagement, training, and workshops This component is divided into the following sub-components:

- **Subcomponent 1(a):** Development of key enablers for whole-of-government approaches: review and support the implementation of personal data protection laws and regulations; assess the cybersecurity baseline; support the implementation of the Pakistan Cloud first policy; develop and support the adoption of an Open Data framework; develop Pakistan Digital Government Institutional Framework; develop Pakistan Digital Government Enterprise Architecture; develop Pakistan Digital Government Data Governance and Interoperability Framework; support nationwide consultation, information sessions, training, and workshops for public sector staff, private sector, and civil society.
- **Subcomponent 1(b)**: Development and Implementation of Interoperability Exchange Layer: stock taking of existing sources of data in the country; building governance and institutional capacity; producing the detailed technical design and procurement documentation for the national data exchange layer; developing the technological infrastructure for the national data exchange layer; writing relevant documentation; and integrating prioritized databases and services.
- **Subcomponent 1(c):** Development of digital authentication, digital vaults, and digital wallets: define the most appropriate architecture for the digital authentication services; identify key services to be provided by the digital identification and authentication solution; deploy the prioritized services for the use of digital authentication; and creation of personal data vaults including feasibility, design and deployment, and awareness campaigns etc.
- **Subcomponent 1(d)**: National Digital Portal and Digital Services Collaboration: conducting an inventory of services; mapping business processes and regulations; providing advice on transitioning systems to cloud infrastructure; producing detailed technical designs and procurement documentation; developing new systems; and supporting knowledge transfer
- **Subcomponent 1(e)**: **Civic Innovation** includes design testing, communications and outreach, digital inclusion for women and girls, and the Digital Government Fellowship. It promotes innovative, data-driven services through an open data and regulatory sandbox; targeted multi-lingual outreach to underserved and rural communities; women's digital literacy pilots in all provinces implemented through public-private partnerships, including support for GBV-related digital services; a Digital Government Innovation Program providing grants to youth and start-ups for citizen-centric digital services at federal and provincial levels; and change management and capacity-building in the public sector. Overall, the subcomponent strengthens public-sector capacity, advances social and gender outcomes, and supports resilient, data-driven digital governance, including in times of crisis.
- **Component 2**: Pakistan Business Portal. This component will support the BoI to modernize regulatory regimes in Pakistan at three levels of government: federal, provincial, and municipal.

The first stage entails reviewing, mapping, and developing a catalogue of registrations, certificates, licenses, and others (RLCOs) across the three levels of the government, potentially including up to 800 government agencies relevant to dealing with investing and operating businesses in Pakistan. Activities for establishment of PBP will include stock taking and reform recommendation for simplifying, streamlining, and improving existing regulatory requirements for investing and operating business across Pakistan; digitalization of compliance with regulatory approvals; institutionalizing the reform process as well as the management and upgradation of PBP; and Communicating reforms and transitions to PBP.

Component 3: Project management. This component will cover the establishment of Project Management Units (PMU).

3. Assessment of Gender Related Risk

The DEEP Project operates in a digital environment where existing gender gaps in access, skills, and decision-making can translate into heightened exposure of women and vulnerable groups to digital exclusion, misuse of data, online harassment, and related risks. These risks require deliberate safeguards to ensure that digital transformation under DEEP remains inclusive, safe, and equitable.

3.1. IDENTIFICATION AND MITIGATION OF RISK

While DEEP does not involve physical infrastructure, the scale of its Digital Public Infrastructure (DPI) introduces context-specific gender risks linked to platform design, data governance, grievance handling, and user engagement. Without appropriate controls, women and marginalized users may face increased vulnerability to digital abuse, privacy violations, TFGBV, SEA/SH, and exclusion from digital services, as well as risks during in-person outreach, facilitation, and civic innovation activities.

To address these risks, DEEP has undertaken a structured gender risk assessment covering digital access, identity systems, data exchange, grievance redress mechanisms, innovation platforms, and in-person engagements. Risk levels and mitigation measures have been identified and integrated into system design, operational protocols, and institutional arrangements, ensuring survivor-centered safeguards, accountability, and continuous monitoring.

The detailed gender-specific risks and corresponding mitigation measures are presented in the table below, providing a clear framework for gender-responsive implementation and risk management across all DEEP components.

Table 1: Identification of gender related risks and required mitigation measures.

Sr. #	Gender-Specific Risk	Risk Level	Mitigation Measure
1	**Under-representation of women in digital policy formulation, safeguards governance, and DPI decision-making**	High	• Institutionalized inclusion of women experts, women-led CSOs, academia, and gender specialists in digital policy consultations, safeguards review committees, and interoperability governance under DEEP • Mandatory gender-lens review of digital policies, SOPs, interoperability agreements, and safeguards frameworks (Digital ID, NDEL, CSP, PBP, Wallets/Vaults) • Documentation and disclosure of women's representation in policy processes for accountability
2	**Gendered information, literacy, and awareness gaps across digital use, consent, and reporting pathways**	High	• Local-language, pictorial, and audio digital literacy content covering onboarding, consent, fraud prevention, and reporting • In-app tutorials and step-by-step guidance on safe use, data sharing, and complaint submission • Community-level outreach with women-led CSOs, including rural and underserved districts

			• Clear, repeated in-portal explanations of survivor rights, confidentiality, and reporting options
3	**Reduced control of women over digital access due to shared devices, SIMs, or mediated access**	High	• Discreet login/logout, session timeout, and safe-exit features across CSP, PBP, Digital ID, and wallets • Device-change alerts, access notifications, and activity visibility for users • Gender-responsive verification and recovery support for women facing access disputes or credential loss • Targeted digital safety literacy on shared-device risks
4	**Higher exposure of women to cyber harassment, fraud, impersonation, blackmailing, doxing, and technology-facilitated GBV across DPI platforms**	**High**	• Integrate dedicated, encrypted complaint plug-ins within the Citizen Services Portal (CSP) and Pakistan Business Portal (PBP) that clearly separate technical/service grievances from sensitive and/or digital harm complaints (cyber harassment, fraud, impersonation, blackmailing, doxing, TFGBV, SEA/SH). • Enable automatic, system-based routing (without manual handling) of sensitive complaints via in-app plug-ins to the designated grievance or investigation modules of NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, relevant Ombudsperson Offices, Police Cyber Units, and other legally mandated authorities, based on complaint type and jurisdiction. • Apply end-to-end encryption**,** survivor-controlled data sharing, role-based access controls, and audit trails to ensure that technical teams, service staff, or unrelated personnel cannot access, intercept, or process sensitive complaint data. • Embed clear digital safety guidance and reporting information within CSP, PBP, and civic platforms to promote safe participation and informed reporting by women and vulnerable users.
5	**Risk of harassment, intimidation, or inappropriate behavior during in-person DEEP activities (trainings, outreach/awareness, civic innovation)**	High	• Enforced Codes of Conduct for all staff, contractors, facilitators, mentors, and partners • Mandatory SEA/SH, cyber-harassment, and professional conduct training prior to deployment • Presence of trained female facilitators/guider and supervisors where culturally appropriate • Clear, confidential reporting and escalation mechanisms at all physical engagements
6	**Lower participation of women in civic innovation labs, competitions, and seed-grant programs due to safety and representation barriers**	Medium - High	• Gender-inclusive outreach strategies and competition design • Safe participation protocols and moderation for in-person and online activities • Structured mentoring, onboarding, and capacity-building for women innovators • Gender-balanced juries, mentors, evaluators, and facilitation teams
7	**Indirect profiling or targeting of women and vulnerable groups**	Medium	• Gender- and vulnerability-sensitive dataset screening and anonymization prior to publication

	through misuse or misinterpretation of open datasets		• Risk-based reviews to prevent re-identification, inference of sensitive attributes, or spatial/temporal profiling • Enforced ethical data-use guidelines and Terms of Use for civic innovation and research activities • Monitoring of dataset access, usage patterns, and feedback loops
8	**Fear of retaliation, stigma, or exposure discouraging women from reporting digital harms**	High	• Anonymous reporting options with survivor-controlled notification settings (no default alerts to shared devices or third parties) • Clear communication of confidentiality protections and non-retaliation safeguards • Trusted reporting channels integrated within CSP/PBP and outreach campaigns with women-led organizations
9	**Invisibility of persons with disabilities and gender-vulnerable groups in DPI design and facilitation**	Medium -High	• Inclusive mapping and needs assessments covering PWDs, transgender persons, elderly women, and other vulnerable groups • Accessibility-by-design features (screen readers, text-to-speech, simplified navigation, contrast modes) • Mitigate accessibility barriers by integrating user training modules within the portal, supported by facilitation staff during the awareness and initial guidance phase. • Engagement of representative organizations in testing, design review, and feedback

4. Gender Action Plan: Addressing DPI-Related Gender Risks and Strengthening Online Harassment Response Mechanisms

The Project will carry out a number of focused and targeted measures to prevent and lessen the gender-related risks mentioned in the preceding section and to promote a more inclusive and gender-responsive digital transformation. Table 3 (GAP) below provides specifics on these measures.

SECTION 1: DIGITAL PUBLIC INFRASTRUCTURE (DPI): GENDER, DIGITAL SAFETY, CYBER RISK & DATA MISUSE ACTION MATRIX

Component	Output / Outcome	Objectives	Indicators of Project Result	Required Actions / Activities / Initiatives	Responsibility	Timeline
Digital Policies, Legal & Safeguards Ecosystem (Cross-Cutting DPI Governance)	Gender-responsive, inclusive, and enforceable digital governance and safeguards framework across all DEEP DPI components	• To ensure meaningful and sustained representation of women and gender-vulnerable groups in digital policy formulation, review, and safeguards oversight • To apply a gender and safety lens to all DPI-related laws, regulations, SOPs, MoUs, interoperability frameworks, and institutional arrangements • To strengthen institutional accountability for prevention and response to TFGBV, cyber harassment, impersonation, fraud, doxing, and data misuse	• Number of DPI-related policies, regulations, or frameworks developed or amended to include gender-responsive digital safety and TFGBV provisions • Percentage of SOPs, MoUs, ToRs, and legal instruments revised to include tech-GBV, cyber-risk, confidentiality, and data-misuse clauses • Number and percentage of women represented in policy review committees, technical working groups, and safeguards oversight mechanisms under DEEP • Completion of documented gender-lens legal reviews for Digital ID, NDEL, Digital	• Establish formal, gender-inclusive policy and safeguards committees under DEEP, including women experts, women-led CSOs, legal practitioners, and digital-rights specialists • Conduct systematic gender-lens legal and regulatory reviews of DPI laws, interoperability agreements, and safeguards instruments (Digital ID, NDEL, wallets/vaults, CSP, PBP) • Revise and harmonize SOPs, MoUs, ToRs, procurement documents, and operational manuals to embed safeguards against TFGBV, cyber harassment, impersonation, fraud, doxing, and data misuse • Define and institutionalize minimum gender-responsive digital safeguards standards applicable across all PIUs and DPI platforms	Health/Gender/Safety Consultant (PMU–MoITT); Legal & Policy Teams (PMU & PIUs); Gender Specialists or E&S Focal Persons (Citizen Services, Civic Innovation, NADRA, BOI); Relevant DPI Technical Leads (PIUs)	Y2–Y5

			Wallets/Vaults, CSP, and PBP frameworks	• Facilitate structured consultations with women users, gender experts, and vulnerable groups at key policy drafting and review stages • Maintain documented records of representation, decisions, and safeguards outcomes to support transparency, disclosure, and audit		
Citizen Services Portal (CSP), Pakistan Business Portal (PBP), Digital ID, Digital Wallets & Vaults	Women are able to safely control, use, and recover their digital accounts without coercion, dependency, or misuse	• To reduce loss of control arising from shared devices, shared SIMs, or assisted access • To enable independent, secure, and dignified access for women across all DPI platforms • To prevent impersonation, unauthorized access, and account misuse during both self-service and assisted interactions	• Percentage of women using secure authentication, session-control, and safety features • Number and percentage of account access and recovery cases resolved for women users • Reduction in complaints related to impersonation, unauthorized access, or account misuse • Percentage of women reporting confidence in account safety and control	• Enable discreet login/logout, safe-exit options, and session-timeout controls across CSP, PBP, Digital ID, and wallet/vault interfaces • Implement device-change alerts, access notifications, and user-visible activity logs to detect misuse • Establish secure, gender-sensitive verification and recovery pathways for women facing loss of access, impersonation, or credential disputes • Integrate digital literacy and in-app guidance on safe account access, fraud prevention, and risks associated with shared devices or assisted use • Ensure assisted services follow clear SOPs on consent, confidentiality, and non-interference	Health/Gender/Safety Consultant (PMU–MoITT); Technical & Development Teams of CSP, PBP, Digital ID & Wallets (NADRA, BOI, Citizen Services Team - PIUs); Gender & E&S Focal Persons (NADRA, BOI, Citizen Services Team)	Y2–Y5
Citizen Services Portal (CSP), Pakistan Business Portal (PBP), Digital ID, Digital Vault and Wallet	Increased onboarding, sustained participation, and active transactions by women across DPI platforms	• To improve representation of women in registrations and digital transactions • To reduce procedural, literacy-related, and facilitation-related barriers to onboarding and use	• Percentage increase in women registrations across CSP, PBP, Digital ID, and Digital Vault & Wallet • Sex-disaggregated transaction volumes and frequency of use • Number and percentage of women-led SMEs and	• Design and implement targeted outreach and awareness campaigns for women users and women-led SMEs (urban and rural) • Simplify onboarding journeys through guided walkthroughs, local-language prompts, and low-literacy user flows	Health/Gender/Safety Consultant (PMU–MoITT); Technical & Development Teams of CSP, PBP, Digital ID, Digital Vault/Wallet & NDEL (NADRA, BOI, Citizen Services Team - PIUs); Gender Specialist	Y2–Y5

		• To enable safe, informed, and independent participation during both self-service and assisted interactions	business entities on boarded through PBP • Percentage of women reporting ease, safety, and confidence in onboarding and service use	• Establish sex-disaggregated monitoring dashboards to track registrations, usage, and drop-off points across DPI platforms • Provide women-focused facilitation windows and mobile outreach, where culturally appropriate, with clear SOPs on informed consent and non-interference • Integrate orientation modules on safe digital use, fraud prevention, and available grievance/reporting pathways	and/or E&S Focal Persons (NADRA, BOI, Citizen Services Team)	
Citizen Services Portal (CSP), Pakistan Business Portal (PBP), Civic Platforms & Competitions – Secure Digital Safety & Complaint Architecture	Safe, confidential, and survivor-centered digital participation environment supported by secure complaint handling and institutional coordination	• To reduce women's exposure to cyber harassment, fraud, impersonation, doxing, blackmailing, TFGBV and SEA/SH across DPI platforms • To clearly separate sensitive digital harm complaints from routine technical service grievances • To ensure encrypted, anonymous, and survivor-centered complaint intake and routing without interception or misuse	• Percentage of sensitive complaints submitted through encrypted CSP/PBP channels • Percentage of sensitive complaints automatically routed via system plug-ins (no manual handling) • Zero incidents of unauthorized access, interception, or data leakage • Percentage of cases handled within defined SLA timelines • User safety and confidentiality satisfaction scores (women and gender-vulnerable users)	• Deploy dedicated, encrypted complaint-handling plug-ins within CSP and PBP that explicitly distinguish technical service grievances from sensitive digital harm complaints • Apply end-to-end encryption, anonymization, survivor-controlled data sharing, role-based access controls, and audit trails to all sensitive complaints • Enable automatic, system-based routing (without manual intervention) of sensitive complaints to the designated grievance or investigation modules of NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, relevant Ombudsperson Offices, Police Cyber Units and/or other relevant entities/agencies based on complaint type and jurisdiction	Health/Gender/Safety Consultant (PMU–MoITT); Technical & Development Teams of CSP, PBP, Digital ID & NDEL (PIUs); Gender Specialist and/or E&S Focal Persons (Citizen Services, NADRA, BOI, Civic Innovation); Institutional Coordination Interfaces with NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units and or other relevant agencies	Y2–Y5

				• Embed digital safety guidance, reporting prompts, and safe-participation warnings across CSP, PBP, civic platforms, forums, and competitions • Introduce platform moderation protocols and Codes of Conduct for civic platforms and competitions • Maintain centralized, anonymized dashboards within CSP/PBP for trend analysis and SLA monitoring without exposing survivor identities		
Trainings, Outreach & Civic Innovation Engagements (In-Person Activities)	Safe, respectful, and well-governed in-person participation environments for women and gender-vulnerable groups	• To Prevent harassment, intimidation, coercion, or inappropriate behavior during field engagements (outreach and awareness campaign and other project activities) • To ensure dignified, voluntary, and informed participation of women and vulnerable groups • To reduce SEA/SH and power-imbalance risks in project-supported events	• Percentage of staff, facilitators, mentors, contractors, and partners trained on Codes of Conduct (CoC) and SEA/SH protocols • Number and percentage of SEA/SH or misconduct incidents reported and resolved through project GRM • Results of compliance checks and supervision audits conducted during trainings, outreach, and innovation events	• Enforce project-wide Codes of Conduct applicable to all staff, consultants, contractors, event partners, mentors, and volunteers involved in trainings, outreach, and civic innovation activities • Mandatory SEA/SH, cyber-harassment, and professional conduct training prior to deployment for any role involving participant interaction • Deployment of female facilitators and supervisors, where culturally appropriate, during trainings, outreach, competitions, and innovation activities • Establish clear, visible, and confidential reporting mechanisms at venues, including anonymous options and survivor-centered response protocols • Implement immediate response, documentation, referral, and disciplinary procedures for any	Health/Gender/Safety Consultant (PMU–MoITT); Civic Innovation Team; Gender Specialist and/or E&S Focal Persons (relevant PIUs); Communication, Coordination and Outreach Team of project (PMU & PIUs), Event Management and Facilitation Teams	Y2–Y5

				violations, linked to the project GRM and SEA/SH action framework		
Civic Innovation Labs, Competitions & Seed Grants (Ignite)	Increased, safe, and meaningful participation of women innovators across civic innovation ecosystems	• To address safety, mobility, and representation barriers faced by women innovators • To promote inclusive, respectful, and well-governed innovation spaces • To enable women's equitable access to mentorship, funding, and visibility	• Percentage of women participants across labs, competitions, hackathons, and seed-grant programs • Number and percentage of women-led ideas, prototypes, or startups supported • Retention and completion rates of women participants • Participant feedback scores (women) on safety, inclusion, fairness, and support	• Design and implement gender-inclusive outreach strategies, including partnerships with women-led CSOs, universities, incubators, and community networks • Integrate Codes of Conduct, anti-harassment provisions, and participant safeguards into competition rules, seed-grant guidelines, and lab operations • Establish safe participation protocols for both in-person and virtual activities, including moderation, reporting pathways, and survivor-centered response mechanisms • Provide structured mentorship, onboarding, and capacity-building support for women innovators (technical, business, and digital safety aspects) • Ensure gender-balanced juries, mentors, evaluators, and facilitation teams to reduce bias and improve fairness in selection and evaluation	Health/Gender/Safety Consultant (PMU–MoITT); Civic Innovation Team (Ignite PIU); Gender Specialist and/or E&S Focal Persons (Civic Innovation Team and relevant PIUs); Partner Organizations and Event Management Teams	Y2–Y5
Open Data Portal & Civic Platforms	Ethical, gender-sensitive, and harm-preventive use of public datasets	• To prevent indirect profiling, re-identification, or harmful inference affecting women and gender-vulnerable groups • To promote responsible, inclusive, and rights-	• Percentage of datasets reviewed and anonymized using gender- and vulnerability-sensitive criteria • Number of awareness and capacity-building sessions	• Apply gender- and vulnerability-sensitive dataset screening and anonymization standards prior to publication on the Open Data Portal • Conduct risk-based reviews to prevent re-identification, inference of sensitive attributes, or	Health/Gender/Safety Consultant (PMU–MoITT); Civic Innovation Team (Ignite PIU); Technical Teams Managing the Open Data Portal (Citizen-Develop Program Lead); Gender	Y2–Y5

		respecting data use across civic platforms • To ensure open data supports innovation without enabling gender-based harm	conducted on responsible data use • Number of reported concerns or incidents related to dataset misuse or harmful inference • Feedback from women users and researchers on data safety and usability	spatial/temporal profiling of women and vulnerable groups • Develop and enforce ethical data-use guidelines and Terms of Reference (ToRs) for civic challenges, research use, and third-party access • Deliver targeted awareness and capacity-building sessions on responsible data use, ethical analytics, and prevention of gender-based harm • Monitor dataset access patterns, reuse cases, and user feedback to identify misuse risks and trigger corrective actions	Specialist and/or & E&S Focal Persons (Civic Innovation team and relevant PIUs)	
CSP, PBP & Awareness / Communication Channels	Increased awareness, trust, and safe use of digital reporting mechanisms by women and gender-vulnerable users	• To increase informed and safe reporting of cyber harassment, fraud, impersonation, and digital exploitation by women • To reduce fear, stigma, retaliation, and misuse of reporting mechanisms • To ensure women understand where, how, and when to report sensitive digital harms	• Percentage increase in cyber-risk and harassment reports submitted by women (sex-disaggregated) • Reach and frequency of awareness campaigns (SMS, radio, social media, in-app) • Percentage of women correctly identifying reporting pathways (survey or feedback-based) • Reduction in incomplete or abandoned complaint submissions by women	• Design and implement gender-responsive IEC and awareness campaigns through SMS, radio, community media, and in-app messaging on CSP and PBP • Embed clear, step-by-step reporting guidance within CSP and PBP interfaces using simple language, icons, and local languages • Partner with women-led CSOs, community networks, and outreach teams to reach rural and underserved women • Clearly communicate confidentiality safeguards, anonymity options, and survivor-controlled follow-up mechanisms	Health/Gender/Safety Consultant (PMU–MoITT); Communication, Coordination & Outreach Teams of NADRA, BOI & Citizen Services Team-PIUs; Gender & E&S Focal Persons (Citizen Services and Civic Innovation Team -PIUs)	Y2–Y5

				• Ensure no default notifications to family members, employers, or third parties without explicit user consent		
All DPI Components (CSP, PBP, Digital ID, NDEL, Digital Wallets/Vaults, Civic Innovation Platforms) - Persons with Disabilities (PWDs) & Gender-Vulnerable Groups	Inclusive, safe, and dignified access to digital and assisted DPI services for PWDs and gender-vulnerable users	• To reduce gender- and disability-based exclusion from digital public services • To improve representation of PWDs and gender-vulnerable groups in DPI design, testing, and service delivery • To ensure accessibility and safety during both self-service and assisted interactions	• Number and percentage of PWDs and gender-vulnerable users accessing DPI services (sex- and disability-disaggregated) • Accessibility compliance indicators across portals, apps, and facilitation points • User satisfaction and usability feedback from PWDs and gender- vulnerable groups • Number of DPI features or services revised based on accessibility feedback	• Conduct systematic inclusive mapping and needs assessments covering women with disabilities, transgender persons, elderly women, and other vulnerable groups prior to and during DPI rollout • Integrate accessibility-by-design features across portals and apps (screen readers, text-to-speech, simplified navigation, high-contrast modes, keyboard-only access) • Ensure accessible assisted services at facilitation centers (trained staff, alternative formats, physical accessibility, privacy-respecting support) • Engage representative organizations of PWDs and gender-vulnerable groups in user testing, design reviews, and feedback loops • Monitor disaggregated participation data and complaints to identify exclusion patterns and trigger corrective system improvements	Health/Gender/Safety Consultant (PMU–MoITT); All PIUs (Citizen Services, NADRA, BOI, Civic Innovation); Gender Specialist and/or E&S Focal Persons form all PIUs; Technical & UX Teams of DPI Platforms (PMU abd PIUs)	Y2–Y5

SECTION 2: ONLINE HARASSMENT COMPLAINT SYSTEMS: CURRENT GAPS AND THE STRENGTHENED DIGITAL PORTAL - CSP & PBP

Component / Gap Area	Output / Outcome	Objectives	Indicators of Project Result	Required Actions / Activities / Initiatives	Responsibility	Timeline
Fragmented and Unsafe Digital Harm Reporting Pathways	Single, trusted, and secure digital entry point for online harassment and cyber harm complaints	• To eliminate fragmented, informal, or unsafe reporting routes for online harassment and digital harms • To increase women's confidence to report cyber harassment, fraud, impersonation, doxing, and TFGBV • To ensure all sensitive complaints enter a controlled, encrypted, and auditable system	• Percentage of online harassment and cyber harm complaints submitted through CSP • Reduction in complaints reported via informal or unverified channels • Women-disaggregated trust and confidence scores on reporting safety	• Designate CSP as the sole project-managed digital intake gateway for sensitive digital harm complaints (cyber harassment, fraud, impersonation, doxing, TFGBV) • Embed secure GRM plug-ins within CSP and PBP to enable portal-specific complaint submission through dedicated interfaces The plug-ins separate routine service issues from sensitive digital harm complaints and ensure automated, non-manual processing within each portal • Implement clear intake separation at entry point, distinguishing routine technical service grievances from sensitive digital harm complaints • Configure complaint-type mapping within CSP and PBP so sensitive complaints are automatically routed - via encrypted system plug-ins - to the legally competent authority modules (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, relevant Ombudsperson Offices, Police Cyber Units and/or other relevant agencies), without CSP and PBP staff access to complaint content • Publish high-level in-portal disclosure ("Where your complaint goes") explaining automated routing and confidentiality safeguards, without revealing investigative workflows	Health/Gender/Safety Consultant from PMU–MoITT; Gender Specialist and/ or E&S Specialist from all PIUs (more importantly-Citizen Services and BoI - PIUs); Technical & GRM Teams in Citizen Services and BoI (PIUs); System-level coordination interfaces with NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, and Police Cyber Units (as receiving authorities via secure plug-ins)	Y3–Y5
Fear of Retaliation and Loss of Privacy	Confidential, survivor-controlled reporting	• To reduce women's fear of retaliation from family members,	• Percentage of sensitive complaints submitted	• Enable anonymous reporting by default for all sensitive digital harm categories, with survivor choice to disclose identity at later stages	Health/Gender/Safety Consultant from PMU–MoITT; Gender Specialist and/or E&S Specialist from	Y2–Y4

	environment for sensitive digital harm complaints	employers, community actors, or perpetrators • To prevent secondary harm arising from visibility, traceability, or unauthorized disclosure of complaints • To enable discreet, anonymous, and survivor-controlled reporting of cyber harassment, fraud, impersonation, doxing, and TFGBV	anonymously through CSP/PBP • Percentage of users selecting survivor-controlled notification and follow-up options • Reduction in abandoned or withdrawn complaints (women-disaggregated) • Women-disaggregated satisfaction scores on privacy, confidentiality, and safety	• Implement survivor-controlled notification settings, ensuring no default SMS, email, or app notifications are sent to shared devices or third parties without explicit consent • Apply data minimization and masked identifiers within CSP/PBP so complaint content and personally identifiable information are not visible to technical, helpdesk, or non-authorized staff • Configure controlled disclosure at referral stage, ensuring that only the minimum necessary data fields are transmitted via encrypted plug-ins to the competent authority based on complaint type and jurisdiction • Provide clear in-portal guidance explaining privacy safeguards, consent choices, non-retaliation principles, and safe use of the reporting system	all PIUs (more importantly-Citizen Services and BoI – PIUs); Legal & Privacy Teams (PMU); Technical & GRM Teams of Citizen Services and BoI (PIUs); Gender Specialist and/or E&S Focal Persons; Competent Authorities (NCCIA, PTA, Police Cyber Units, relevant Ombudsperson Offices, MoHR/NCHR/NCSW/ NCRC as applicable) as secure receiving endpoints bound by agreed confidentiality and data-protection protocols	
Non-Survivor-Centered Intake and Triage Practices	Trauma-informed, gender-sensitive intake and triage for sensitive digital harm complaints	• To improve dignity, trust, and psychological safety for women complainants at first point of contact • To reduce under-reporting and early drop-off of cyber harassment, fraud, impersonation, doxing, and TFGBV complaints • To ensure respectful, confidential, and consistent handling	• Percentage of sensitive complaints handled by staff trained in trauma-informed, survivor-centered protocols • Percentage of women complainants requesting and receiving female intake or triage support (where operationally feasible) • Women-disaggregated satisfaction scores on	• Mandatory trauma-informed and survivor-centered training for all CSP/PBP GRM and helpdesk staff handling sensitive digital harm complaints • Availability of female intake and triage support options (digital or in-person), where operationally feasible and appropriate • Standardized intake and triage SOPs covering informed consent, confidentiality, non-retaliation, respectful communication, data minimization, and clear referral boundaries • Anonymous intake and discreet follow-up options, allowing complainants to control communication mode and timing • Periodic quality assurance reviews of intake practices to ensure compliance with survivor-centered standards	Health/Gender/Safety Consultant from PMU–MoITT; Gender Specialist and/or E&S Specialist from all PIUs (more importantly-Citizen Services and BoI – PIUs); Legal & Privacy Teams from PMU and PIUs; Citizen Services GRM & Technical Teams (PIUs); (No operational role for NCCIA, PTA, Police Cyber Units, Ombudsperson Offices, or other external agencies at intake/triage stage - engagement occurs only post-	Y2–Y4

		before automated referral	dignity, safety, and confidentiality at intake stage		referral via automated system plug-ins)	
Unsafe Handling of Sensitive Complaint Data	Secure, non-intercept able, and survivor-protected management of sensitive digital harm complaint data	• To prevent unauthorized access, interception, or secondary misuse of sensitive complaints • To protect complainant anonymity, confidentiality, and data integrity end-to-end • To ensure technical operations, system maintenance, and helpdesk functions cannot access sensitive complaint content	• Zero incidents of unauthorized access, data leakage, or interception • Percentage of sensitive complaints processed exclusively through encrypted channels • Percentage of access events compliant with defined role permissions • Successful completion of periodic security audits and penetration tests	• End-to-end encryption and anonymization for all sensitive complaint categories (cyber harassment, fraud, impersonation, doxing, TFGBV) from intake through referral • Strict role-based separation between system administrators/technical operations and complaint intake, review, and routing functions • Masked identifiers and data minimization, ensuring personally identifiable information is visible only to authorized complaint-handling roles when strictly necessary • Tamper-proof audit logs capturing all access, actions, and transfers within the complaint module • Targeted security testing (vulnerability assessments and penetration testing) focused specifically on complaint-handling components • Secure API / connector controls for automated plug-ins, including endpoint whitelisting, cryptographic keys, token rotation, logging, and monitoring • No manual data export, screenshots, email forwarding, or off-system access permitted at any stage	Health/Gender/Safety Consultant from PMU–MoITT; Gender or E&S Specialist from all PIUs (more importantly- Citizen Services and BoI –PIUs); CSP/PBP Technical Architecture & Security Teams (PMU and PIUs); Legal & Privacy Focal Persons Competent Authorities' IT endpoints only (NCCIA, PTA, Police Cyber Units, Ombudsperson Offices, etc.) as secure receiving systems bound by agreed encryption, access-control, and logging standards (no access by their operational staff outside their own systems)	Y2–Y5
Unclear or Delayed Routing to Competent Authorities	Predictable, automated, and survivor-safe routing of sensitive digital harm complaints to legally mandated authorities	• To ensure timely, consistent, and non-discretionary referral of complaints • To eliminate manual handling, ad-hoc decisions, or discretionary routing	• Percentage of sensitive complaints automatically routed via system plug-ins • Average time from intake to system-generated referral	• Configure automated routing plug-ins from CSP to the grievance/investigation modules of NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, relevant Ombudsperson Offices, and Police Cyber Units, based on complaint category and jurisdiction • Implement rule-based routing logic with no discretionary override by operational or technical staff	Health/Gender/Safety Consultant from PMU–MoITT; Gender Specialist and/or E&S Specialist from all PIUs (more importantly- Citizen Services and BoI –PIUs); CSP/PBP Technical & Architecture Teams (PIUs) Formal coordination	Y3–Y5

		• To protect survivor confidentiality and safety during referral and escalation	• Percentage of referrals meeting defined SLAs • Zero incidents of manual forwarding or off-system data sharing	• Enforce system-generated referrals only (no emails, screenshots, downloads, or data copying outside CSP/PBP) • Apply survivor-controlled data sharing, transmitting only the minimum necessary fields to each authority • Maintain SLA monitoring dashboards, routing logs, and automated failure/latency alerts to flag delays or transmission issues	interfaces with NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, and Police Cyber Units (as secure receiving/mandated entities bound by agreed technical and confidentiality standards)	
Weak Case Tracking and Follow-Up Visibility	Transparent, time-bound case tracking within DEEP systems with safe referral-status visibility	• To prevent loss, duplication, or stagnation of sensitive digital harm complaints • To enable predictable, time-bound responses across intake, referral, and closure stages • To strengthen internal accountability without exposing survivor identities or investigation details	• Percentage of complaints meeting defined timelines for intake, referral, and closure • Average time from intake to first recorded system action • Percentage of escalations resolved within prescribed timeframes • Percentage of complaints with current status visible to complainants (masked)	• Implement centralized, role-based case-tracking dashboards within CSP using masked identifiers and data minimization • Define and enforce standard SLAs and escalation thresholds for each stage (intake, routing, acknowledgement, closure) • Enable system-generated alerts and reminders for overdue actions, stalled cases, and unresolved escalations • Configure automated acknowledgement and high-level status signals from competent authority plug-ins (e.g., received / under review / closed), without transmitting investigation content or personal data back to CSP • Restrict visibility of dashboards to authorized roles only; prohibit manual notes on authority-side actions • Conduct periodic internal case-flow reviews to identify bottlenecks, SLA breaches, and systemic delays, and document corrective actions	PMU - MoITT; CSP/PBP Technical & GRM Teams (PIUs); Gender Specialist and/or E&S Focal Persons from all PIUs; Competent Authorities (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units) (limited to automated acknowledgement and status signals via secure plug-ins)	Y2–Y4
Limited Learning from Digital Harm Trends	Institutionalized, evidence-based improvement of CSP/PBP online harassment	• To identify emerging and recurring patterns of online harassment, cyber fraud, impersonation,	• Quarterly analytical reports on digital harm complaints produced and reviewed	• Conduct gender-disaggregated analysis at CSP/PBP system level covering complaint types, intake drop-off points, routing timelines, SLA compliance, and closure outcomes (without accessing investigation content)	Monitoring & Evaluation Team (PMU and PIUs); Health/Gender/Safety Consultant (PMU–MoITT) Gender Specialist and/or E&S Focal Person from all PIUs;	Y2–Ongoing

	complaint systems	doxing, and TFGBV affecting women • To continuously strengthen intake design, safeguards, routing efficiency, and survivor protections • To ensure complaint systems remain adaptive to evolving digital harm risks and user behaviors	• Number of intake, routing, or safeguard updates informed by analysis • Functioning gender-disaggregated dashboards covering complaint categories, timelines, and outcomes • Documented reduction in repeat, delayed, or unresolved complaint patterns over time	• Produce quarterly analytical briefs highlighting trends, systemic bottlenecks, confidentiality risks, and user experience gaps • Convene structured learning reviews involving GRM teams, technical teams, and gender specialists to translate findings into concrete system improvements • Update intake forms, user guidance, routing rules, SLA thresholds, and safeguard features based on evidence and survivor feedback • Share aggregated, non-identifiable trend insights with competent authorities (NCCIA, PTA, Police Cyber Units, Ombudsperson Offices, etc.) solely to improve coordination, routing logic, and plug-in performance, not for case-level follow-up • Track implementation of recommended improvements and document follow-up actions for audit and accountability	CSP/PBP Technical & GRM Teams (PIUs); Competent Authorities (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units) (limited to coordination on aggregated trends and plug-in performance; no access to identities or case data)	

5. Monitoring, Evaluation, Learning and Reporting Framework

The Monitoring, Evaluation, Learning, and Reporting (MELR) framework under the DEEP Gender Action Plan (GAP) is a core accountability and learning mechanism designed to ensure gender-responsive, safe, and inclusive participation across all Digital Public Infrastructure (DPI) components supported by the project. The MELR framework systematically tracks, evaluates, and responds to gender-differentiated digital risks, including online harassment, cyberbullying, fraud, impersonation, doxing, blackmail, identity theft, personal data misuse, technology-facilitated gender-based violence (TFGBV), and SEA/SH (in-person engagement under project), while also monitoring women's access, participation, and leadership across DEEP-supported platforms and programs.

The framework supports continuous adaptive management by translating evidence into improvements in system design, safeguards, policies, operational protocols, outreach strategies, and institutional coordination. It strengthens transparency, accountability, and learning across all implementing entities, including:

- Citizen Services Portal (CSP)
- Pakistan Business Portal (PBP)
- National Data Exchange Layer (NDEL)
- Digital ID and Digital Vaults/Wallets
- Open Data Portal
- Civic Innovation Platforms, Labs, Competitions, and Seed Grant Programs

The MELR framework aligns with the World Bank Environmental and Social Framework (ESF), the World Bank Gender Strategy (2024–2030), and DEEP's E&S safeguards architecture, ensuring compliance with ESS1, ESS2, ESS4, ESS10, and gender commitments.

To ensure ground-level inclusion and responsiveness, the MELR framework integrates both:

- Quantitative monitoring (gender- and vulnerability-disaggregated indicators), and
- Qualitative insights (beneficiary feedback, survivor experience, field observations, and institutional learning).

5.1. OBJECTIVES OF THE MELR FRAMEWORK

The MELR framework is designed to achieve the following objectives:

- Monitor gendered digital risks across all DEEP platforms, including online harassment, cyberbullying, fraud, impersonation, doxing, identity theft, data misuse, TFGBV, and SEA/SH-related digital complaints.
- Track women's participation, access, and retention across Digital Public Infrastructure (CSP, PBP, Digital ID, Digital Vault/Wallets, NDEL-enabled services), civic innovation programs, competitions, seed grants, and assisted access mechanisms.

- Assess effectiveness of gender risk mitigation measures, including anonymous and survivor-controlled reporting, encrypted complaint handling, trauma-informed intake, and consent-based routing mechanisms.
- Identify participation gaps and exclusion risks affecting women, persons with disabilities (PWDs), transgender persons, low-literacy users, and other vulnerable groups across digital and assisted services.
- Enable adaptive, evidence-based system improvements by using monitoring data and feedback to refine platform design, safeguards, policies, SOPs, training modules, and outreach strategies.
- Strengthen institutional accountability and coordination by generating actionable, non-identifiable insights for PMU, PIUs, and coordination with competent authorities (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units and/or other relevant agencies).
- Ensure compliance with World Bank ESF and DEEP safeguards, while preserving survivor confidentiality, data integrity, and clear separation between project monitoring and statutory enforcement functions.

5.2. KEY ELEMENTS: GENDER MELR FRAMEWORK:

1. **Gender-Disaggregated and Risk-Sensitive Monitoring**

All DEEP digital platforms will systematically collect gender-disaggregated and vulnerability-sensitive data to monitor participation gaps and digital risks, while strictly applying confidentiality, anonymization, and data-minimization principles.

This monitoring will include:

- User characteristics: women, men, transgender persons, persons with disabilities (PWDs), rural/urban users, low-literacy users, and shared-device users.
- Participation and transaction metrics across CSP, PBP, Digital ID, Digital Vault/Wallet NDEL-Enabled Services, Civic Innovation Labs, Competitions, Open Data Portals and DEEP-supported seed-grant programs.
- DPI-associated risks and harms: online harassment, cyberbullying, fraud, impersonation, blackmail, doxing, identity theft, and misuse of personal or business data.
- TFGBV and SEA/SH-related digital complaints: number received, automatically routed, resolved, survivor satisfaction, and confidentiality compliance (tracked only in anonymized form).
- Adoption of proactive safety features: usage of anonymous reporting, survivor-controlled notifications, consent mechanisms, and secure evidence upload tools.

Anonymized analytical tools - including trend analysis, heat maps, and risk dashboards - will be used to identify emerging threats and inform targeted mitigation actions at platform and community levels.

2. **Integrated Dashboards for Real-Time Monitoring**

A centralized, role-based digital monitoring dashboard will be embedded across CSP, PBP, and relevant DPI systems to support real-time monitoring, evaluation, and decision-making.

Dashboards will provide:

- Anonymized real-time visibility of online harassment, cyber fraud, impersonation, blackmail, data misuse, and TFGBV trends.
- Gender-disaggregated participation metrics, including:
    - Registrations, logins, and transactions by women and vulnerable groups.
    - Participation of women in civic innovation programs, competitions, and seed-grant initiatives.
- Complaint system performance indicators, including intake-to-routing timelines, SLA compliance, and system-generated status acknowledgements (without exposure of investigation or authority-level details).
- Adoption metrics for consent, privacy, security, and survivor-controlled features across platforms.

Access to dashboards will be strictly restricted to authorized PMU and PIU roles, ensuring survivor confidentiality and system integrity.

3. High-Quality Independent Evaluation

Independent evaluation is integral to the MELR framework to ensure credibility, accountability, and impact validation.

This includes:

- Annual third-party audits assessing compliance with data-privacy rules, cyber-safety standards, gender inclusion commitments, and digital safeguards.
- Midline and end-line impact evaluations assessing the effectiveness of mitigation measures across Digital ID, NDEL, CSP, PBP, the Open Data Portal, Civic Innovation Activities-CITL, Seed Grants, and Outreach & Awareness Programs.
- Independent verification of CSP and PBP complaint system performance, focusing on timeliness, survivor-centered handling, confidentiality safeguards, and user trust.
- Technology and algorithm audits to detect bias, privacy gaps, or vulnerabilities in authentication, data-exchange, or automated routing mechanisms.

Evaluation findings will directly inform corrective actions, protocol updates, and system redesigns.

4. Learning Reviews and Adaptive Management

DEEP institutionalizes continuous learning and adaptive management to respond to evolving digital risks.

Key mechanisms include:

- Quarterly learning reviews involving PMU, PIUs, Gender/E&S Specialists/Focal Person, and technical system teams.
- Structured coordination sessions with NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, and Police Cyber Units and/or related agencies - limited strictly to aggregated, non-identifiable trends and system-performance insights.
- Annual protocol updates covering:
    - Digital harassment and fraud reporting workflows
    - Secure evidence handling
    - Consent and privacy management
    - Gender-responsive UX, accessibility, and inclusion standards
- Development of IEC materials (visual, audio, and low-literacy formats) in collaboration with women-led CSOs to strengthen awareness of digital rights, digital literacy, prevention strategies, and reporting mechanisms.

This approach ensures dynamic risk management and system adaptability without compromising survivor safety or confidentiality.

5. Participatory Feedback Mechanisms

Women's experiences and voices are central to MELR implementation.

Participatory mechanisms include:

- Confidential, in-portal feedback surveys capturing user safety, usability, trust, and accessibility concerns.
- Focus group discussions (FGDs) with women, PWDs, transgender persons, rural users, and low-literacy groups.
- Engagement with women-led CSOs and NGOs to assess UX, outreach effectiveness, and community-level inclusion.
- Feedback-to-action loops, ensuring user input directly informs platform design, training modules, outreach strategies, and safeguard enhancements.

6. Alignment with DEEP Results Framework and ESF

All MELR indicators and activities are fully aligned with:

- DEEP Results Framework and Project Operational Manual (POM)
- Environmental and Social Framework (ESF) and Environmental and Social Commitment Plan (ESCP)
- World Bank Gender Strategy, SEA/SH Good Practice Note, and Digital Development guidance

Key tracked outcomes include:

- Increased, safer, and sustained participation of women across DEEP digital public infrastructure (DPI) platforms, including CSP, PBP, Digital ID, Digital Vault/Wallet, Civic Innovation Platforms, and innovation ecosystems.
- Expanded adoption and effective use of digital safety, data-protection, privacy, and consent-management features across all DEEP platforms.
- Timely, automated, and confidential handling of cyber-harm complaints through system-embedded GRM plug-ins, with performance monitored via defined SLAs, audit logs, and anonymized outcome indicators.
- Reduced risks of TFGBV across digital platforms through secure system design, privacy safeguards, and safe reporting mechanisms.
- Reduced risks of SEA/SH during in-person project engagements (trainings, outreach, consultations, and civic innovation activities) through enforced Codes of Conduct, trained staff, and confidential reporting and escalation mechanisms.
- Meaningful inclusion of women in digital governance, policy formulation, and innovation ecosystems across DEEP components, including decision-making, design, and oversight processes.

7. Reporting and Institutional Accountability

Robust reporting mechanisms ensure transparency and accountability:

- Quarterly reports on participation, digital-risk trends, complaint-system performance, and mitigation effectiveness.
- Annual consolidated GAP implementation reports, including lessons learned and corrective actions.
- A dedicated Health/Gender/Safety Consultant at PMU- MoITT responsible for coordination, quality assurance, and World Bank reporting.
- Gender Specialist and/or E&S Focal Persons in each PIU responsible for implementation, monitoring, and coordination.
- Standardized, gender-disaggregated reporting templates used across PIUs.
- Independent annual reports produced by M&E specialists or third-party monitoring firms.
- Presentation of findings to the Project Steering Committee (PSC) and submission to the World Bank.

8. Knowledge Management and Sustainability

The MELR framework institutionalizes long-term learning and sustainability by:

- Documenting best practices on gender-inclusive digital governance and digital safety.
- Building a gender-focused knowledge repository on digital Literacy, digital Inclusion, digital harassment prevention, safe identity systems, and inclusive innovation.
- Supporting federal–provincial and local alignment on gender-responsive digital policies and governance.

- Ensuring sustainability of DEEP platforms, safeguards, and institutional arrangements beyond project closure.

The Monitoring, Evaluation, Learning, and Reporting (MELR) framework under DEEP transcends conventional tracking by embedding gender accountability, digital safety, survivor protection, and inclusive digital participation across all levels of digital governance. Through real-time analytics, participatory feedback, automated safeguards, and coordinated institutional monitoring, the framework systematically tracks and strengthens women's and vulnerable groups' access, digital literacy, meaningful engagement, and safe use of all Digital Public Infrastructure (DPI) components supported under DEEP. This integrated approach ensures that inclusion, capability-building, and protection remain foundational pillars of Pakistan's digital transformation under the project.

5.3. REPORTING MECHANISM FOR GAP (CONTENTS, RESPONSIBILITY, FREQUENCY, AND RECIPIENTS)

Component / Sub-Component	Contents of Report	Who Will Prepare	Frequency	Recipients
Digital Policies, Legal & Safeguard Ecosystem	• Number and scope of policies, SOPs, MoUs, ToRs, and legal instruments updated to address online harassment, cyber fraud, impersonation, data misuse, doxing, TFGBV, and SEA/SH under project, within DPI environments • Evidence of gender-lens legal and safeguards review applied to Digital ID, NDEL data-exchange frameworks, and digital vaults/wallets (consent, data minimization, misuse-prevention clauses) • Institutionalization of gender-responsive safeguards within digital governance instruments (confidentiality, automated routing, non-retaliation, survivor-controlled reporting) • Women's representation and documented participation in digital-policy consultations, safeguards reviews, and oversight committees under DEEP	Health/Gender/Safety Consultant (PMU–MoITT) in close coordination with Gender Specialists and/or E&S Focal Persons from all PIUs, Project Legal & Policy Team, and M&E Specialist (PMU & PIUs) (for indicator validation and reporting quality assurance)	Quarterly	Program Director - PMU; Project Directors of PIUs; PSC; World Bank Task Team
Women's Participation, Digital Literacy & Safe Use Across DEEP DPI	• Percentage of women users across CSP, PBP, Digital ID, and digital vaults/wallets (disaggregated by urban/rural, assisted vs. self-service access) • Gender-disaggregated usage and transaction patterns, including drop-off points and exclusion signals linked to safety, access control, usability, or literacy barriers • Percentage of women reporting digital fear, hesitancy, or reduced usage due to safety, privacy, harassment, fraud, or retaliation risks (captured through anonymized in-portal feedback and surveys) • Coverage, reach, and effectiveness of digital literacy and awareness campaigns (sessions conducted, participant profiles, geographic coverage, and key learning gaps) • Evidence of gender-lens review of onboarding, authentication, transaction, and literacy workflows to identify unintended exclusion or risk amplification	Health/Gender/Safety Consultant (PMU–MoITT), in close coordination with Gender Specialists and/or E&S Focal Persons from all PIUs; M&E Specialist (indicator design, sex-disaggregated analysis, trend monitoring, and reporting QA); Digital Literacy Campaign Firm (activity reporting and participant data)	Monthly (operational monitoring) Quarterly (consolidated reporting)	Program Director-PMU; PIU Heads; Project Steering Committee (PSC); World Bank Task Team
CSP Interface Safety (Women & Vulnerable Users)	• Percentage of CSP modules compliant with gender-responsive safety UX standards (anonymous reporting, safe-exit buttons, privacy warnings, discreet navigation) • Number and trend of incidents of digital harassment, stalking, misuse, or intimidation triggered during CSP service use (aggregated and anonymized) • Accessibility measures implemented for persons with disabilities (PWDs), low-literacy users, and transgender users (screen readers, text-to-speech, simplified flows, inclusive language, non-binary options)	Health/Gender/Safety Consultant (PMU–MoITT) in close coordination with CSP Technical Teams (NITB), Gender Specialists and/or E&S Focal Persons from NITB Specifically, and M&E Specialist (for UX safety	Monthly (operational monitoring) Quarterly (consolidated reporting)	Program Director-PMU; NITB; Project Steering Committee (PSC); World Bank Team

	• Evidence of usability testing and safety audits incorporating feedback from women and gender-vulnerable users	indicators, trend analysis, verification of accessibility metrics, and reporting quality assurance)		
CSP Digital Harm Reporting & Resolution System	• Aggregated volume and typology of digital harm complaints submitted through CSP/PBP (cyber harassment, fraud, impersonation, blackmail, doxing, TFGBV, SEA/SH) • Percentage of sensitive complaints automatically routed via secure system plug-ins (no manual handling) to competent authorities • Percentage of complaints meeting defined SLAs for intake, routing, acknowledgement, and closure • Compliance with secure evidence handling standards (encrypted uploads, access control, audit logs) • Anonymized survivor satisfaction indicators related to safety, dignity, confidentiality, and trust in the reporting system • Aggregated referral statistics by authority (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units), including receipt confirmation and status signals (no investigation details)	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with CSP/PBP Technical & GRM Teams (PIUs), Gender & E&S Focal Persons, and M&E Specialist –more importantly-Citizen Services Team -PIU (for indicator definition, SLA trend analysis, aggregation, validation, and WB-aligned reporting)	Quarterly	Program Director-PMU; PIU Heads; Project Steering Committee (PSC); World Bank Task Team
NDEL – Interoperability Layer (Gender, Privacy & Safety Compliance)	• Percentage and scope of interoperability agreements, APIs, and data-exchange protocols revised with gender-responsive safeguards (consent-based sharing, data minimization, encryption, misuse prevention) • Number of MoUs, SOPs, and interoperability frameworks updated to prevent profiling, tracking, doxing, identity exposure, and misuse of women's and vulnerable users' data • Number of detected incidents of unauthorized access, re-identification, or misuse of gender-disaggregated or sensitive data via NDEL (Target: 0) • Evidence of gender-lens review of NDEL governance rules, automated exchange logic, and access controls • Aggregated, non-identifiable feedback from women users (especially rural, low-literacy, and underserved groups) on trust, consent clarity, and safety of NDEL-enabled services	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with Gender Specialists and/or E&S Focal Persons from all PIUs (especially from NADRA) , M&E Specialist (indicator tracking and trend analysis), and NADRA (NDEL Lead) technical & legal teams	Quarterly	Program Director-PMU; Project Directors of PIUs (specifically NADRA); PSC; World Bank Task Team
Digital ID, Digital Vaults & Wallets (High-Risk DPI Platforms)	• Results of gender-responsive vulnerability assessments covering identity theft, impersonation, deep fake misuse, SIM-swap risks, coerced access, and unauthorized credential recovery	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with Gender Specialists and/or E&S Focal	Monthly (operational) Quarterly (consolidated)	Program Director - PMU; Project Director - NADRA

	• Aggregated (non-identifiable) number and trend of fraud, impersonation, extortion, or blackmail cases linked to Digital ID, vaults, or wallets (reported via CSP/PBP and auto-routed through plug-ins) • Percentage of women users registered and actively using Digital ID, vaults, and wallets (urban/rural; assisted vs self-service) • Percentage of women users utilizing safety features (secure login, session timeout, device-change alerts, recovery safeguards) • Measures implemented to protect transgender users (mis-gendering, dead-naming, unauthorized disclosure prevention) Evidence of gender-lens review of authentication workflows, recovery processes, and automated decision rules	Persons from all PIUs (especially from NADRA), M&E Specialist (sex-disaggregated monitoring and trend analysis), and NADRA PIU (Digital ID & NDEL Lead)		PIU; PSC; World Bank Task Team
Civic Innovation, Digital Inclusion & Outreach (CITL – Ignite)	• Number and scope of TFGBV, cyber safety, data protection, and ethical innovation modules integrated into CITL labs, competitions, hackathons, and training programs • Percentage and profile of women innovators receiving structured mentoring on digital safety, secure design, data protection, and responsible innovation • Aggregated number and type of reported incidents of harassment, intimidation, or exclusion during in-person or virtual innovation activities (without personal identifiers) • Number and percentage of women-led prototypes, startups, or solutions addressing digital safety, anti-harassment tools, privacy-by-design, safe authentication, anti-doxing, or inclusive DPI features • Participation of rural, low-literacy, and gender-vulnerable women in CITL-supported activities and outreach initiatives.	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with Civic Innovation team- Ignite PIU (CITL Management & Innovation Teams and Firm-Innovation Specialist), Gender Specialist & E&S Focal Persons, and M&E Specialist (for indicator design, participation tracking, trend analysis, and outcome reporting)	Quarterly	Program Director-PMU; Ignite PIU; Project Steering Committee (PSC); World Bank Task Team
Open Data Portal & Ethical Use (Civic Innovation Initiative)	• Percentage and categories of datasets screened, anonymized, or withheld due to gender, vulnerability, or re-identification risks • Aggregated number and type of detected incidents of harmful inference, profiling, or misuse of published datasets (no user or subject identification) • Number and percentage of women researchers, academics, and innovators accessing Open Data Portal resources safely (urban/rural) • Consolidated, non-identifiable feedback from women researchers on data usability, safety, consent clarity, and ethical concerns • Status of policies, SOPs, and governance controls updated to prevent re-identification, sensitive attribute inference, or misuse of gender-disaggregated data	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with Open Data Portal Team - Citizen Develop Program Lead Consultant (Civic Innovation-PIU), Gender Specialist and/or E&S Focal Persons, and M&E Specialist (for dataset screening indicators, misuse trend analysis, feedback synthesis, and compliance reporting)	Semi-Annual	Program Director-PMU; Ignite PIU; Project Steering Committee (PSC); World Bank Task Team

Pakistan Business Portal (PBP) – Digital Safety & Secure Business Engagement for Women	• Results of periodic digital-safety audits of PBP workflows (onboarding, registration, payments, communications) to identify risks of fraud, impersonation, extortion, or harassment affecting women entrepreneurs • Aggregated number and trend of reported cyber fraud, extortion, impersonation, or data-misuse cases linked to PBP services (reported via CSP/PBP and auto-routed through secure plug-ins) • Percentage of women-led businesses reporting harassment-free and safe business engagement through PBP (urban/rural; assisted vs self-service access) • Uptake of safety features and safeguards (secure transactions, privacy warnings, consent prompts, safe exit options) • Number and scope of outreach, awareness, and trust-building activities conducted with women chambers of commerce, business associations, and women-led CSOs, including consolidated feedback from participants (non-identifiable)	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with BOI PIU (PBP Lead), Gender Specialist and or & E&S Focal Persons, and Monitoring & Evaluation (M&E) Specialist (for indicator validation, trend analysis, outreach effectiveness assessment, and consolidated reporting)	Quarterly	Program Director-PMU; BOI PIU; Project Steering Committee (PSC); World Bank Task Team
Gender-Responsive Staffing & Management (PMU & PIUs)	• Percentage and distribution of women in PMU and PIUs, with specific focus on digital safety, cybersecurity, digital governance, GRM, and technical decision-making roles • Number, coverage, and completion rates of mandatory trainings conducted on TFGBV, cyber risks, digital exploitation, data privacy, consent management, and SEA/SH (staff, contractors, consultants) • Percentage of HR, procurement, operations, and consultancy TORs incorporating gender-responsive clauses, digital safety obligations, Codes of Conduct, and SEA/SH prevention requirements • Evidence of enforcement mechanisms: signed Codes of Conduct, reporting pathways, disciplinary actions (aggregated, non-identifiable) • Inclusion of women-led CSOs, academia, transgender and other vulnerable-group representatives in consultations, staffing panels, and advisory or review processes under DEEP	Health/Gender/Safety Consultant (PMU- MoITT) in close coordination with HR & Administration Units/Specialists (PMU & PIUs), Gender Specialists and/or E&S Focal Persons from all PIUs, and Monitoring & Evaluation (M&E) Specialist (for indicator standardization, workforce trend analysis, training effectiveness assessment, and consolidated reporting)	Quarterly (routine monitoring) Annual (consolidated review) Immediate reporting for severe SEA/SH incidents	Program Director - PMU; Heads of PIUs; Project Steering Committee (PSC); World Bank Task Team
Monitoring of Digital Harm & Data Misuse Cases (Across CSP, PBP, DPI)	• Aggregated volume and categorization of digital harm cases (cyber harassment, fraud, impersonation, doxing, blackmail, TFGBV, SEA/SH) reported through CSP/PBP • Case status distribution and timelines across intake, automated routing, authority acknowledgement, and closure (no personal identifiers)	Health/Gender/Safety Consultant (PMU- MoITT), Gender Specialist and/or E&S Focal Person from all PIUs in close coordination with Monitoring & Evaluation (M&E) Specialist, CSP/PBP Technical & GRM	Monthly (operational monitoring) Quarterly (consolidated reporting)	Program Director - PMU; Project Steering Committee (PSC); World Bank Task Team

	• Percentage of cases auto-routed via secure system plug-ins to competent authorities (NCCIA, PTA, MoHR, NCHR, NCSW, NCRC, Ombudsperson Offices, Police Cyber Units) • SLA compliance rates for intake-to-routing and referral acknowledgement • Secure evidence handling compliance (encrypted uploads, access controls, audit logs – compliance metrics only) • Trend analysis identifying emerging digital risks, repeat patterns, bottlenecks, or system-level vulnerabilities (gender-disaggregated where applicable)	Teams (PIUs), (M&E role: indicator design, trend analysis, SLA tracking, and consolidated reporting; no access to case content)		
Learning & Adaptive Management	• Quarterly learning reviews identifying emerging and evolving digital risks affecting women and vulnerable users (e.g., deep fake-enabled abuse, SIM-swap fraud, biometric misuse, AI-driven impersonation) • Evidence-based assessment of the effectiveness of existing safeguards across CSP, PBP, Digital ID, NDEL, vaults/wallets • Record of protocol, SOP, UX, and safeguard updates made in response to evidence (intake design, consent flows, routing rules, access controls) • Summary of cross-platform system improvements adopted (no case-level details) • Documentation of unresolved risks requiring policy or legal action	Health/Gender/Safety Consultant (PMU–MoITT) in close coordination with Monitoring & Evaluation (M&E) Specialist, Policy & Legal Teams, Gender & E&S Focal Persons (PIUs), and CSP/PBP Technical Teams (M&E role: synthesis of trend analysis, effectiveness assessment, and validation of learning outcomes; no access to complaint content)	Quarterly	Program Director - PMU; Project Steering Committee (PSC); World Bank Task Team
Consolidated Reporting (Internal & External)	• Consolidated MELR reports (monthly, quarterly, and annual) covering women's participation, digital risk trends, complaint-system performance, safeguard effectiveness, and mitigation outcomes (aggregated and anonymized) • Anonymized public dashboards integrated with CSP and PBP showing high-level trends on digital harms, complaint resolution timelines, and adoption of safety features (no case-level or identifiable data) • Annual Gender Action Plan (GAP) implementation report documenting progress, challenges, corrective actions, and lessons learned across all DEEP components • Evidence of alignment with DEEP Results Framework, ESF/ESCP, SEA/SH requirements, and World Bank Gender Strategy • Summary of actions taken in response to identified risks, learning reviews, and audit findings	Health/Gender/Safety Consultant (PMU–MoITT) in close coordination with Monitoring & Evaluation (M&E) Specialist, Gender Specialist and/or E&S Focal Persons (PIUs), and CSP/PBP Technical & GRM Teams (M&E role: data consolidation, indicator validation, trend analysis, results reporting; no access to complaint content or survivor identities)	Monthly / Quarterly / Annual	Program Director- PMU; Project Steering Committee (PSC); World Bank Task Team

Table 2: Gender Action Plan (GAP) – Implementation Timeline, Roles, and Stakeholders

GAP Action Area	Target Participants (Head Count)	Frequency (Y2–Y5)	Timeline	Organizing & Technical Responsibility	Event Execution / Logistics	Key Stakeholders
1. Capacity Building, Awareness, Community Engagement & Inclusive Digital Innovation	30–40 per session	12 sessions (3 per year)	Y2–Y5	Health/Gender/Safety Consultant (PMU-MoITT); Gender Specialists and/or E&S Focal Person (PIUs); Civic Innovation Team (PIU); Digital Literacy Focal Persons; CSP/PBP Development & Digital Safety Teams- Communication and Coordination and Outreach team of Project	Event Management Firm / Logistics Teams	Women users (urban/rural); PWDs; transgender persons; civic innovators; women entrepreneurs; CSOs/NGOs; academia; private sector (civic-tech, fin tech); provincial & local government departments (Competent authorities participate for awareness only; no case handling)
2. Survivor-Centered Digital Harm, Cyber-Safety & TFGBV/SEA/SH-Sensitive GRM Strengthening	25–35 per session	8 sessions (2 per year)	Y2–Y5	Health/Gender/Safety Consultant (PMU-MoITT); Gender Specialists and/or E&S Focal Person (PIUs); Legal & Cyber-Safety Experts; GRM System Architects of CSP, PBP and NADRA Component Specifically	Event Management Firm / Logistics Teams	GRM focal persons; women representatives; survivor-support CSOs; legal aid providers; NCCIA; PTA; MoHR; NCHR; NCSW; NCRC; Ombudsperson Offices; Police Cyber Units (role limited to mandate clarification, referral protocols, confidentiality standards)
3. Women's Representation, Digital Inclusion & Safe Participation across DPI	30–40 per session	8 sessions (annual)	Y2–Y5	Health/Gender/Safety Consultant (PMU-MoITT); Gender Specialists and/or E&S Focal Person (PIUs); Civic Innovation Team; Digital Literacy Firm and Focal Persons; Communication, Coordination and Outreach Team of Project	Event Management Firm / Logistics Teams	Women Development Departments; women entrepreneurs & SMEs; rural & underserved communities; transgender & gender-vulnerable groups; CSOs; civic tech labs; academia; private sector
4. Monitoring, Evaluation, Learning & Reporting (MELR) for Gender & Digital Risks	20–25 per session	4 sessions (annual)	Y2–Y5	Health/Gender/Safety Consultant (PMU-MoITT); Gender Specialists and/or E&S Focal Person (PIUs);M&E Specialist from all Units; Digital Risk & Policy Experts)	Event Management Firm / PMU Secretariat	PMU & PIUs; Provincial IT Boards; policy & data units; Gender & E&S experts; NCCIA; PTA; MoHR; NCHR; NCSW; NCRC and other related agencies (participation limited to aggregate trend review and system-level learning)
Total Planned Sessions		**32 Sessions**				

ANNEX A: DEFINITIONS OF KEY TERMINOLOGIES[2]

Terms	Definition
Accountability and Response Framework	The framework details how allegations of SEA/SH are handled (administrative investigation procedures) and how disciplinary actions for violation of the required behaviors by workers are determined, including as set out in any Code of Conduct or Behavioral Standards.
Code of Conduct	In Good Practice Note (GPN), a Code of Conduct (CoC) refers to a written document that sets out core principles and minimum standards of behavior with which project actors agree to comply on an individual basis, specifically in relation to a financed project by World Bank. A CoC will usually be rolled out to individuals who are not covered by existing Behavioral Standards and who are engaged specifically for the project. Violation of the CoC may result in disciplinary action by an employer and may affect the worker's ongoing employment.
Gender-based violence	Gender-based violence (GBV) is an umbrella term for any harmful act that is perpetrated against a person's will and that is based on socially-ascribed (i.e., gender) differences between males and females. It includes acts that inflict physical, sexual, or mental harm or suffering; threats of such acts; coercion; and other deprivations of liberty.
Gender-based violence (GBV) service provider	An organization offering specific services for GBV survivors, including survivors of SEA/SH, such as health services, psychosocial support, shelter, legal aid, safety/security services, etc.
Gender minorities	Individuals whose gender identity/expression does not fit into the distinct categories of male or female, or "cisgender." This encompasses transgender identities, as well as those exhibiting a non-conforming expression of gender. This term includes "third gender" individuals because their identity does not fit into the gender binary.
Sexual Assault	Sexual activity with another person who does not consent. It is a violation of bodily integrity and sexual autonomy and is broader than narrower conceptions of "rape," especially because (a) it may be committed by other means than force or violence, and (b) it does not necessarily entail penetration

[2] Good Practice Note: Addressing SEA/SH in IPF Involving Major Civil Works: https://documents1.worldbank.org/curated/en/099430304232515972/pdf/IDU-0df177e9-284c-4850-bdf5-10a5cb6607b3.pdf

Sexual Exploitation and Abuse (SEA)	**Sexual exploitation**: Any actual or attempted abuse of a position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. **Sexual Abuse**: Actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions. Sexual abuse is a broad term, which includes a number of acts including rape and sexual assault, among others.
Sexual harassment (SH)	Any form of unwanted verbal, non-verbal, or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating, or offensive environment. This may include unwelcome sexual advances, or requests for sexual favors, and may take place through online activity or mobile communications as well as in person.
Survivor-centered approach	The survivor-centered approach is based on a set of principles and skills designed to guide professionals—regardless of their role—in their engagement with survivors (predominantly women and girls but also men, boys, and gender minorities) who have experienced sexual or other forms of violence. The survivor-centered approach aims to create a supportive environment in which the survivor's interests are respected and prioritized, and in which the survivor is treated with dignity and respect. The approach helps to promote the survivor's recovery and ability to identify and express needs and wishes, as well as to reinforce the survivor's capacity to make decisions about possible interventions, including non-intervention. In SEA/SH cases involving children, the survivor-centered approach is guided by an assessment of the best interests of the child.

ANNEX B: CODE OF CONDUCT

This Code of Conduct applies to all workers engaged in the project management and implementation. It highlights the expected standards of professional behavior to ensure a safe, respectful, and inclusive environment for all project stakeholders. The Code specifically commits all individuals to uphold "Zero Tolerance" for SEA/SH throughout the project lifecycle.

Individual Code of Conduct: Preventing Sexual Exploitation and Abuse, Sexual Harassment[3]

I **(full Name of Employee)** acknowledge that preventing any misconduct as stipulated in this code of conduct, including sexual exploitation and abuse (SEA), sexual harassment (SH), and child abuse/exploitation are important. Any activity, which constitute acts of gross misconduct are therefore grounds for sanctions, penalties or even termination of employment. All forms of misconduct are unacceptable be it on the work site or off work. Prosecution of those who commit any such misconduct will be pursued as appropriate. I agree that while working on this project, I will:

1. Consent to security background check;
2. Treat women, children (persons under the age of 18) and persons with disability with respect regardless of race, color, language, religion, political or other opinion, national, ethnic or social origin, property, birth or other status;
3. Not use language or behavior towards men, women or children/learners that is inappropriate, harassing, abusive, sexually provocative, demeaning or culturally inappropriate;
4. Carry out my duties competently and diligently;
5. Comply with this Code of Conduct and all applicable laws, regulations and other requirements, including requirements to protect the health, safety and well-being of other Contractor's Personnel and any other person;
6. Maintain a safe working environment including by:
   a) ensuring that workplaces, machinery, equipment and processes under each person's control are safe and without risk to health;
   b) wearing required personal protective equipment (PPE);
   c) using appropriate measures relating to chemical, physical and biological substances and agents; and
   d) following applicable emergency operating procedures.
7. Report work situations/environment that I believe are not safe or healthy and remove myself from a work situation which I reasonably believe presents an imminent and danger to my life or health;
8. Treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers (if engaged) or children;
9. Not engage in any form of sexual harassment including unwelcome sexual advances, requests for sexual favors, and other unwanted verbal or physical conduct of a sexual nature with other Contractor's or Employer's Personnel;
10. Not participate in sexual activity with children, including grooming or through digital media. Mistaken belief regarding the age of a child and consent from the child is not a defense;

[3] Labor Management Procedure of Digital Economy Enhancement Project (DEEP)

11. Not exchange money, employment, goods, or services for sex, with community members including sexual favors or other forms of humiliating, degrading or exploitative behavior;
12. Attend trainings related to HIV and AIDS, GBV/SEA/SH, occupational health and any other relevant courses on safety as requested by my employer;
13. Report to the relevant committee any situation where I may have concerns or suspicions regarding acts of misconduct by a fellow worker, whether in my company/organization or not, or any breaches of this code of conduct provided it is done in good faith;
14. Regarding children (under the age of 18):

Refrain from hiring children for domestic or other labor, which is inappropriate given their age, or developmental stage, which interferes with their time available for education and recreational activities, or which places them at significant risk of injury.

a) Comply with all relevant local legislation, including labor laws in relation to child labor

15. Refrain from any form of theft for assets and facilities including from surrounding communities.
16. Remain in designated working area during working hours;
17. Refrain from possession of alcohol and illegal drugs and other controlled substances in the workplace and being under influence of these substances on the job and during workings hours;
18. Follow prescribed environmental occupation health and safety standards;
19. Channel grievances through the established grievance redress mechanism.

I understand that the onus is on me to use common sense and avoid actions or behaviors that could be construed as misconduct or breach of this code of conduct.

I acknowledge that I have read and understand this Code of Conduct, and the implications have been explained with regard to sanctions on-going employment should I not comply.

Signed by: _____

Signature: _____

Date: _____

For the Employer/Contractor

Signed by: _____

Signature: _____

Date: _____

ANNEX C: OVERVIEW OF GENDER-FOCUSED LEGISLATION

1. INTERNATIONAL COMMITMENTS

1.1. Convention on the Elimination of all Forms of Discrimination against Women (CEDAW)[4]

Pakistan ratified CEDAW in 1996, which calls upon state parties to condemn discrimination against women in all its forms and places an obligation on states to take all appropriate measures to eliminate such discrimination by any person, organization, or enterprise. The U.N. Committee on the Elimination of Discrimination Against Women (CEDAW Committee), established under CEDAW, has noted that "gender-based violence is a form of discrimination which seriously inhibits women's ability to enjoy rights and freedoms on a basis of equality with men"

1.2. United Nations Convention on the Rights of the Child (UNCRC)[5]

In 1990 Pakistan ratified UNCRC, and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography in 2011. UNCRC obligates State Parties to protect children from all forms of sexual exploitation and sexual abuse and take measures to prevent: a) the inducement or coercion of a child to engage in any unlawful sexual activity; (b) exploitative use of children in prostitution or other unlawful sexual practices; (c) exploitative use of children in pornographic performances and materials.

2. NATIONAL LAWS

2.1. Protection Against Harassment of Women at the Workplace (Amendment) Act, 2022

The Protection against Harassment of Women at the Workplace Act, 2022 introduced amendments in the previous Act of 2010, and has further broadened its scope. The Act defines harassment as (a) "any unwelcome sexual advance, request for sexual favors, stalking or cyber stalking, or other verbal, visual or written communication or physical conduct of a sexual nature, or sexually demeaning attitudes, including any gestures or expression conveying derogatory connotation causing interference with work performance or creating an intimidating, hostile or offensive work environment, or the attempt to punish the complainant for refusal to comply to such a request or is made a condition for employment"; and (b) "discrimination on the basis of gender which may or may not be sexual in nature, but which may embody discriminatory and pre-judicial mind set or notion, resulting in discriminatory behavior on basis of gender against the complainant"[6].

Upon receiving a complaint, the employer is required to set up an Inquiry Committee consisting of three members, of which one must be a female. The complainant also has the option to complain

---

[4] UN Committee on the Elimination of Discrimination Against Women (CEDAW): https://www.refworld.org/legal/resolution/cedaw/1992/en/96542

[5] Convention on the Rights of the Child: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[6] THE PROTECTION AGAINST HARASSMENT OF WOMEN AT WORKPLACE (AMENDMENT) ACT. 2022: https://www.commerce.gov.pk/wp-content/uploads/2022/02/Protection-Against-Harassment-of-Women-at-WorkPlace-Act-2022.pdf

directly to the Ombudsperson. If the Inquiry Committee finds the accused to be guilty, it can impose penalties such as censure; withholding for a specific period promotion or increment; recovery of the compensation payable to the complainant from pay or any other source of the accused; reduction to a lower post; compulsory retirement; and removal from service.

2.2. Prevention of Anti-Women Practices (Criminal Law Amendment) Act, 2011

The law defines and prohibits certain practices that may lead to exploitation and discrimination against womenfolk. The practices defined and prohibited in the Act include:

• **Prohibition of depriving women from inheriting property**: Those denying women of their movable or immovable properties at the time of opening of succession shall be punished with imprisonment of either description for a term which may extend to ten years but not be less than five years or with a fine of one million rupees or both.

• **Prohibition of forced marriage**: Those who coerce women in any manner to enter into marriage shall be punished with imprisonment of either description for a term, which may extend to ten years or for a term which shall not be less than three years and shall also be liable to fine of five hundred thousand rupees.

• **Prohibition of marriage with the Holy Quran**: Those who compel or facilitate the marriage of a woman with the Holy Quran shall be punished with imprisonment of either description which may extend to seven years which shall not be less than three years and shall be liable to a fine of five hundred thousand rupees.

Relevance of this act with DEEP: The Prevention of Anti-Women Practices Act, 2011 underpins DEEP's dedication to gender equality and digital inclusion by establishing a legal framework for safeguarding women's rights, especially with inheritance, marriage, and protection against detrimental traditional practices. DEEP's digital platform can be utilized to augment awareness of these fundamental safeguards, permit the reporting of violations, and facilitate access to legal assistance. under employing inclusive design and integrating with legal referral systems, DEEP has the capacity to enhance women's legal empowerment and mitigate the incidence of exploitative activities addressed under this Act.

2.3. PECA 2016 and Amendment 2025: Gender and Digital Safety Provisions[7]

Pakistan's gender-responsive digital protection regime is grounded in the Prevention of Electronic Crimes Act, 2016 (PECA), which provides legal safeguards against online harms that disproportionately affect women and girls. Key gender-relevant provisions include Section 20 (Offences Against Dignity), Section 21 (Cyberstalking), Section 22 (Unauthorized Use of Identity Information), Section 24 (Sexual Harassment), and Section 37 (Unlawful Online Content), each

[7] Government of Pakistan. *Prevention of Electronic Crimes Act, 2016 (Act No. XL of 2016):* https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

addressing forms of technology-facilitated gender-based violence such as non-consensual image sharing, blackmail, impersonation, and digital harassment. The digital governance framework was strengthened through the Prevention of Electronic Crimes (Amendment) Act, 2025[8], which consolidates essential components of the earlier E-Safety Bill, 2023, including enhanced content moderation, improved takedown mechanisms, and expanded authority of federal institutions responsible for digital safety oversight. Together, these Acts establish a more comprehensive and gender-sensitive legislative framework designed to improve online safety, strengthen accountability mechanisms, and protect women and vulnerable populations in Pakistan's digital ecosystem.

2.4. Pakistan Penal Code, 1860: Section 376: Punishment for Rape

Under Section 376 of the Pakistan Penal Code, 1860 amended under the Criminal Law Amendment Act, 2020; any person who commits rape will be punished with death or life imprisonment without parole till death, and will also be liable to a fine. Similarly, in the case of gang rape, where two or more persons are involved, the punishment for each person is death or life imprisonment without parole till death.

2.5. Other Provisions in the Pakistan Penal Code, 1860[9]

- Under Section 509 of the Pakistan Penal Code, if a person insults a woman regarding her modesty, whether through gestures or words, the perpetrator can be charged with three years of imprisonment, or with a fine, or both.
- Under Section 496C of the Pakistan Penal Code, anyone making false accusations against another female is to be punished with five years in prison and with a fine.
- A person who does something that is considered indecent and vulgar, including singing or reciting a song with vulgar lyrics, shall be liable under Section 354A of the Pakistan Penal Code and shall be imprisoned for three months or may be given a fine or be ordered to do both.
- A person who assaults a woman, uses physical force against her, or strips her of her clothes for the public to see, may be given a death sentence or imprisoned for life, under Section 354A of the Pakistan Penal Code.
- A person who forces a young girl under the age of 18 to have sexual intercourse with another person, will be charged with 10 years of imprisonment or with a fine under Section 366A of the Pakistan Penal Code.

[8] Government of Pakistan. *Prevention of Electronic Crimes (Amendment) Act, 2025:* https://na.gov.pk/uploads/documents/679255ee36f45_595.pdf

[9] Anti-Harassment Laws in Pakistan: https://courtingthelaw.com/2019/06/10/commentary/anti-harassment-laws-in-pakistan/