Ministry of Information Technology, Communication and Innovation

# DIGITAL TRANSFORMATION IMPLEMENTATION PLAYBOOK

**VERSION 0.1 — LIVING DOCUMENT** | Published: March 2026

# Executive Preface

## *Digital Transformation Implementation Playbook*

Operational Companion to the National AI Strategy and FAIR Guidelines

### Three Documents. One Programme.

Since December 2025, the AI Unit of the Ministry of Information Technology, Communication and Innovation has operated with a clear mandate: to lead the responsible adoption of Artificial Intelligence across the public service of the Republic of Mauritius.

Three documents define this programme. Together they form a complete architecture from principle to practice:

| | | |
|---|---|---|
| **WHAT** | **National AI Strategy (AIM)** | The strategic vision. What Mauritius is building: the objectives, pillars, and outcomes that define responsible AI adoption for the nation. |
| **WHY** | **FAIR Guidelines** | The ethical foundation. Why our approach to AI is grounded in Fairness, Accountability, Inclusivity, and Responsibility - the values that govern every decision. |
| **HOW** | **This Playbook** | The operational methodology. How AI pilots will be designed, delivered, governed, and evaluated - the frameworks, processes, and standards that turn strategy into outcomes. |

### A Hypothesis in the Right Direction

This document is published deliberately and is deliberately incomplete.

> ***"A playbook written before delivery begins is a hypothesis. A playbook updated after delivery begins is a weapon."***

Version 0.1 represents the best operational thinking available before the first pilot run. It draws on internationally recognised frameworks: CRISP-DM, ITIL, WCAG 2.2, and Kirkpatrick and maps them to the Mauritian public service context. It is coherent, principled, and directionally correct.

It is also, by definition, untested. Sections on failure protocols, on what to do when a pilot underperforms and on how to navigate real constraints of data availability and institutional

capacity, these will be written with authority only after we have encountered those situations. That is as it should be.

Readers should approach this document accordingly: as a rigorous starting framework, not a finished manual. Every practitioner who uses it is contributing to the next version.

## What Version 0.1 Contains

- **Part 1 —** Purpose, scope, and how this playbook relates to the Blueprint and the two companion documents above.
- **Part 2 —** Operational delivery frameworks: CRISP-DM for AI pilot delivery, ITIL for service operations, WCAG 2.2 for accessibility, and data governance procedures.
- **Part 3 —** The capability development system: how ministry staff will build skills through structured workshops, mentoring, pair working, and communities of practice, measured through the Kirkpatrick framework.
- **Part 4 —** Delivery governance: RACI matrices, ministry counterpart responsibilities, and vendor management protocols.
- **Part 5 —** Implementation templates and tools (core structures defined; full templates to be published in the National Knowledge Repository, see below).

## What Will Be Added Before the First Pilot Begins

In the interest of transparency, the following elements are acknowledged as forthcoming. They are preconditions for moving from this published framework to live operational delivery:

| Item | Status | Notes |
|---|---|---|
| National Knowledge Repository (NKR) — setup, population of core templates, and access provisioning for Ministry counterparts | **In Progress** | Templates are defined in Part 5. The NKR must be live and accessible before practitioners can begin pilots. |
| Pilot failure and exit protocols — go/no-go decision trees, stage-gate criteria, and escalation templates for underperforming pilots | **Forthcoming** | Will be drafted once the pilot scope and Ministry counterparts are confirmed. Critical pre-condition for pilot launch. |
| Ministry Readiness Assessments — formal verification of counterpart availability, data readiness, and management commitment before each pilot is approved | **Forthcoming** | Assessment template to be developed alongside the first pilot selection process. |
| Playbook v0.2 — incorporating lessons from the first completed pilot cycle | **Planned** | Target: within 60 days of first pilot evaluation completion. |

## Document Ownership and Update Commitment

This playbook is owned by the AI Unit, Ministry of Information Technology, Communication and Innovation. The AI & Data Governance Pod within the Central Digital Delivery Unit is responsible for maintaining and updating it.

**Update schedule:** This document will be formally reviewed and updated following the completion of each pilot cycle. Minor amendments may be made at any time and will be recorded in the version history. The current version is always the operative version.

**Feedback:** Practitioners who identify gaps, errors, or improvements in this document are encouraged to submit feedback to the AI Unit. Contributions from the field are the primary mechanism through which this playbook will improve.

---

**AI Unit**
Ministry of Information Technology, Communication and Innovation
March 2026

# DIGITAL TRANSFORMATION IMPLEMENTATION PLAYBOOK

Operational Companion to AI in Action

**Prepared by:** Ruben Ramdhony

**In support of:** FAIR Guideline

**Date:** March 2026

**GOVERNMENT OF MAURITIUS**
Ministry of Information Technology, Communication and Innovation

CONFIDENTIAL

# Table of Contents


Executive Summary

Part 1: Understanding This Playbook

- 1.1 Purpose and Scope
- 1.2 Relationship to the Digital Transformation Blueprint
- 1.3 Who Should Use This Playbook
- 1.4 How to Navigate This Document

Part 2: Operational Delivery Frameworks

- 2.1 AI & Data Pilot Delivery: CRISP-DM Methodology
- 2.2 Service Operations: ITIL-Aligned Framework
- 2.3 Accessibility Compliance: WCAG 2.2 Implementation
- 2.4 Data Governance Operations

Part 3: Capability Development System

- 3.1 Multi-Layered Learning Model
- 3.2 Kirkpatrick Evaluation Framework
- 3.3 Knowledge Transfer Mechanisms

Part 4: Delivery Governance & Collaboration

- 4.1 Expanded RACI Matrix
- 4.2 Ministry Counterpart Responsibilities
- 4.3 Vendor & Delivery Partner Management

Part 5: Implementation Templates & Tools

- 5.1 Service Design Templates
- 5.2 AI & Data Templates
- 5.3 Training & Knowledge Transfer Templates
- 5.4 Governance Templates

Appendices

- Appendix A: CRISP-DM Detailed Process Guide
- Appendix B: ITIL Process Workflows
- Appendix C: WCAG 2.2 Compliance Checklist
- Appendix D: Kirkpatrick Measurement Instruments
- Appendix E: Glossary of Terms

# Executive Summary

This Implementation Playbook provides the operational frameworks, delivery methodologies, and practical templates needed to execute the strategic vision outlined in the National AI Strategy and FAIR guidelines. It translates high-level governance frameworks into day-to-day execution practices for the AI Unit (AIU) and delivery partners.

The Digital Transformation Blueprint establishes a comprehensive 12-month roadmap for implementing digital government across Mauritius, grounded in internationally recognised frameworks including OECD Digital Government principles, GovStack building blocks, Estonia's X-Road interoperability model, UK GDS Service Standards, and robust AI governance through NIST AI RMF, EU AI Act principles, and ISO 42001.

While the Blueprint provides strategic direction and governance architecture, this playbook addresses the practical question: "*How do we actually implement this on the ground?*"

> **Key Deliverables of This Playbook:**
>
> - CRISP-DM methodology for structured AI and data pilot delivery
> - ITIL-aligned service operations framework for sustainable post-deployment management
> - WCAG 2.2 accessibility implementation guidelines and testing protocols
> - Kirkpatrick-based capability development and measurement system
> - Expanded RACI matrices showing detailed phase-by-phase responsibilities
> - Ready-to-use templates for service design, data governance, training, and quality assurance
> - Knowledge transfer mechanisms including pair working, mentoring, and communities of practice

This playbook is designed to be used alongside the main Blueprint as a practitioner's reference guide. Every section explicitly references the corresponding Blueprint section it operationalises, ensuring continuity and alignment with the strategic vision.

# Part 1: Understanding This Playbook

## 1.1 Purpose and Scope

The purpose of this Implementation Playbook is to bridge the gap between strategic intent and operational execution. It provides the detailed processes, methodologies, templates, and tools that practitioners need to translate the National Digital Transformation Blueprint into tangible outcomes.

### What This Playbook Covers

- **Delivery Methodologies:** Step-by-step processes for implementing AI pilots, designing digital services, and managing operations
- **Quality Standards:** Specific technical standards (WCAG 2.2), testing protocols, and acceptance criteria
- **Capability Building:** Detailed training approaches, mentoring structures, and competency measurement frameworks
- **Governance Mechanics:** Expanded RACI matrices, escalation procedures, and decision-making workflows
- **Practical Templates:** Ready-to-use forms, checklists, and documentation standards

### What This Playbook Does Not Cover

- Strategic rationale and policy frameworks (covered in the main Blueprint)
- High-level governance structures and committee formations (covered in Blueprint Section 4)
- International framework descriptions (covered in Blueprint Section 2)
- Budget allocation and procurement strategy (separate Ministry documents)

## 1.2 Relationship to the Digital Transformation Blueprint

> **Integration Principle:**
>
> This playbook is not a standalone document. It must be read in conjunction with the National AI Strategy and the FAIR guidelines. Every section of this playbook explicitly references the corresponding Blueprint section it operationalises.

The relationship can be understood as follows:

| Blueprint Component | What It Provides | Playbook Complement |
|---|---|---|
| Strategic Objectives | Vision, principles, international frameworks | Not duplicated — reference only |
| 12-Month Roadmap | Phase structure, high-level deliverables | Phase-specific implementation guides and templates |
| Team Structure | Pod definitions, roles, governance tiers | Detailed RACI, counterpart expectations, collaboration protocols |
| Standards & Frameworks | Strategic frameworks (OECD, GovStack, NIST AI RMF) | Operational methodologies (CRISP-DM, ITIL, WCAG 2.2, Kirkpatrick) |
| Capability Building | Training as a roadmap activity | Blended learning model, measurement framework, knowledge transfer mechanics |

## 1.3 Who Should Use This Playbook

This playbook is designed for multiple audiences involved in implementing the Digital Transformation Blueprint:

### Primary Users

#### Central Digital Delivery Unit (CDU) Pods

- **AI & Data Governance Pod:** Use Part 2.1 (CRISP-DM) and Part 2.4 (Data Governance Operations)
- **Service Design & UX Pod:** Use Part 2.3 (WCAG 2.2) and Part 5.1 (Service Design Templates)
- **Digital Architecture & Interoperability Pod:** Use Part 2.2 (ITIL Operations) and Part 4.3 (Vendor Management)
- **Cybersecurity & Resilience Pod:** Use Part 2.2 (Service Operations) and Part 4.1 (RACI)

#### Ministry Digital Focal Points (DFPs)

Ministry focal points should use this playbook to:

- Understand their specific responsibilities in pilot implementations (Part 4.2)
- Prepare their teams for training and knowledge transfer activities (Part 3)
- Coordinate with CDU pods using the RACI framework (Part 4.1)
- Access templates for service design and data governance (Part 5)

### Secondary Users

- **Delivery Partners & Vendors:** Understanding quality expectations, knowledge transfer obligations, and collaboration protocols
- **Architecture & Interoperability Review Board (AIRB):** Reference for technical assurance and compliance verification
- **AI Oversight & Risk Governance Committee:** Understanding operational implementation of AI governance principles
- **Ministry Technical Liaisons:** Day-to-day coordination with CDU pods and implementation teams

## 1.4 How to Navigate This Document

This playbook is structured to support both sequential reading and selective reference:

> **For First-Time Readers:**
>
> Read sequentially through Parts 1-4 to understand the complete operational framework. Use Part 5 and Appendices as reference material during actual implementation.

> **For Practitioners Implementing Specific Activities:**
>
> Jump directly to the relevant section based on your current task:
>
> - Implementing an AI pilot → Part 2.1 (CRISP-DM)
> - Setting up service operations → Part 2.2 (ITIL)
> - Testing for accessibility → Part 2.3 (WCAG 2.2)
> - Designing training programmes → Part 3
> - Clarifying roles and responsibilities → Part 4.1 (RACI)
> - Needing templates or checklists → Part 5

### Cross-Referencing Convention

Throughout this playbook, references to the Digital Transformation Blueprint use the following notation:

→ *Blueprint Section X.X* indicates the corresponding section in the main roadmap document.

# Part 2: Operational Delivery Frameworks

*This section operationalises the Standards, Frameworks & Methodology outlined in Blueprint Section 3 and the Implementation Phases described in Blueprint Section 3.*

## 2.1 AI & Data Pilot Delivery: CRISP-DM Methodology

*→ Operationalises Blueprint Phase 2 (Months 4-8): "Ministry-Level Pilot Implementations" and integrates with AI governance frameworks established in Blueprint Section 2.*

### Purpose and Context

The Digital Transformation Blueprint establishes comprehensive AI governance through NIST AI Risk Management Framework, EU AI Act principles, and ISO 42001. These frameworks provide the strategic governance and risk management approach for AI adoption across government.

This section provides the complementary **delivery methodology** for actually implementing AI and data pilots described in Phase 2 of the Blueprint. CRISP-DM (Cross-Industry Standard Process for Data Mining) serves as the standard operational lifecycle for moving from use case identification to production deployment.

> **Integration with Blueprint Governance:**
>
> CRISP-DM is not a replacement for NIST AI RMF or ISO 42001 — it is the practical delivery process that implements their requirements. Each CRISP-DM phase includes explicit checkpoints for governance compliance, risk assessment, and AIRB technical assurance.

### Why CRISP-DM?

- **Internationally Recognised:** Proven methodology used in government AI implementations globally
- **Framework Alignment:** Maps naturally to NIST AI RMF phases (Govern → Map → Measure → Manage)
- **Quality Gates:** Provides clear checkpoints that integrate with AIRB technical reviews
- **Reproducibility:** Ensures all pilots follow an auditable, repeatable process
- **Risk Management:** Embeds risk assessment and mitigation at every stage

### The CRISP-DM Lifecycle

CRISP-DM consists of six phases arranged in a cyclical process:

### Phase 1: Business Understanding

**Objective:** Define the problem, success criteria, and alignment with ministry objectives

**Key Activities:**

- Document use case and business objectives
- Define success metrics and acceptance criteria
- Conduct stakeholder analysis
- Identify constraints and assumptions
- Assess AI risk level (per EU AI Act classification)

**Governance Checkpoint:**

- Use case approval by AIRB
- Initial AI risk assessment by AI Oversight & Risk Governance Committee
- Alignment with national priorities confirmed by Steering Committee

**Deliverables:**

- Use Case Definition Document (Template in Part 5.2)
- AI Risk Classification Matrix
- Stakeholder Map
- Success Metrics Dashboard Design

**Ministry Counterpart Role:** Lead problem definition, provide business context, validate success criteria

### Phase 2: Data Understanding

**Objective:** Assess data availability, quality, and suitability for the AI use case

**Key Activities:**

- Identify and access relevant data sources
- Perform initial data quality assessment
- Conduct exploratory data analysis
- Verify data governance and privacy compliance
- Document data limitations and risks

**Governance Checkpoint:**

- Data classification per National Data Governance Standard (→ Blueprint Phase 1B)
- Privacy impact assessment if handling personal data
- Data sharing agreement approval (if cross-ministry)

**Deliverables:**

- Data Readiness Assessment Report (Template in Part 5.2)
- Data Quality Scorecard
- Privacy Impact Assessment (if applicable)
- Data Dictionary and Metadata Catalogue

**Ministry Counterpart Role:** Provide data access, validate data interpretation, confirm privacy compliance

### Phase 3: Data Preparation

**Objective:** Transform raw data into analysis-ready datasets

**Key Activities:**

- Data cleaning and quality remediation
- Feature engineering and transformation
- Data integration from multiple sources
- Training/validation/test dataset creation
- Version control and lineage tracking

**Governance Checkpoint:**

- Data lineage documentation (for auditability)
- Bias assessment in training data
- Security review of data storage and access

**Deliverables:**

- Cleaned and Transformed Datasets
- Data Preparation Scripts (version controlled)
- Feature Engineering Documentation
- Bias Assessment Report

**Ministry Counterpart Role:** Validate data transformations, confirm business logic correctness

### Phase 4: Modeling

**Objective:** Develop, train, and validate AI/ML models

**Key Activities:**

- Select appropriate modeling techniques
- Train multiple candidate models
- Perform hyperparameter optimization
- Validate model performance on test data
- Assess model explainability and interpretability

**Governance Checkpoint:**

- Model performance against success criteria
- Explainability assessment (per NIST AI RMF "Measure" phase)
- Fairness and bias testing
- Technical review by AI & Data Governance Pod

**Deliverables:**

- Trained Model(s) with version control
- Model Performance Report (Template in Part 5.2)
- Model Explainability Documentation
- Fairness and Bias Assessment

**Ministry Counterpart Role:** Validate model outputs make business sense, participate in explainability review

### Phase 5: Evaluation

**Objective:** Comprehensively assess whether the model meets all requirements

**Key Activities:**

- End-to-end user acceptance testing
- Performance testing under realistic conditions
- Security and resilience testing
- Accessibility testing (per WCAG 2.2 — see Part 2.3)
- Risk reassessment and mitigation planning

**Governance Checkpoint:**

- AIRB technical assurance review and sign-off
- AI Oversight Committee approval for deployment
- Confirmation of National Digital Service Standard compliance (→ Blueprint Phase 3A)
- User research validation with Service Design & UX Pod

**Deliverables:**

- User Acceptance Testing Report
- Performance Benchmark Results
- Security Assessment Certificate
- Go/No-Go Recommendation

**Ministry Counterpart Role:** Lead user acceptance testing, provide deployment approval

### Phase 6: Deployment

**Objective:** Launch the AI solution into production with monitoring and support

**Key Activities:**

- Production environment setup
- Model deployment and integration
- User training and documentation
- Monitoring dashboard configuration
- Handover to operations team (per Part 2.2 ITIL framework)

**Governance Checkpoint:**

- Final deployment approval by Steering Committee
- Operational readiness verification by Cybersecurity & Resilience Pod
- Knowledge transfer completion confirmed
- Continuous monitoring plan activated (per NIST AI RMF "Manage" phase)

**Deliverables:**

- Production-Ready AI System
- User Documentation and Training Materials
- Operations Runbook (Template in Part 5.2)
- Monitoring and Alerting Configuration
- Model Registry Entry with full lifecycle metadata

**Ministry Counterpart Role:** Receive knowledge transfer, assume operational ownership

## CRISP-DM RACI Matrix

The following table shows detailed responsibilities for each CRISP-DM phase:

| CRISP-DM Phase | AI Unit Expert | Ministry DFP/Staff | CDU AI Pod | AIRB | AI Oversight Committee |
|---|---|---|---|---|---|
| **Business Understanding** | R | R, A | C | I | I |
| **Data Understanding** | R | R (data access) | C | I | I |
| **Data Preparation** | R | C (validation) | C | I | I |
| **Modeling** | R | C (business validation) | C, A (technical review) | I | I |
| **Evaluation** | R | R (UAT lead) | C | C (technical assurance) | A |
| **Deployment** | R | R (receive handover), A | C | C | I |

*R = Responsible (performs the work); A = Accountable (final authority); C = Consulted (provides input); I = Informed (kept updated)*

## Success Criteria for AI Pilots

All AI pilots must meet the following criteria before proceeding to production deployment:

- ☐ Business objectives clearly defined and validated by ministry leadership
- ☐ Data quality assessed at minimum "fit for purpose" standard
- ☐ Model performance meets or exceeds agreed success metrics
- ☐ Explainability documentation provided for all decisions/predictions
- ☐ Fairness and bias testing completed with acceptable results
- ☐ Security assessment passed with no critical vulnerabilities
- ☐ Accessibility testing passed per WCAG 2.2 AA (Part 2.3)
- ☐ User acceptance testing completed with ministry staff
- ☐ AIRB technical assurance review approved
- ☐ AI Oversight Committee deployment approval received
- ☐ Knowledge transfer completed and verified
- ☐ Operational runbook and monitoring configured

## 2.2 Service Operations: ITIL-Aligned Framework

*→ Operationalises Blueprint Phase 3 (Months 9-12): "Institutionalisation, Resilience & National Scale-Up" and supports the Cybersecurity & Resilience Pod responsibilities defined in Blueprint Section 4.*

### Purpose and Context

The Digital Transformation Blueprint establishes the strategic foundations for building digital services through GovStack building blocks, X-Road interoperability, and UK GDS service standards. These frameworks focus primarily on **designing and building** digital government services.

This section provides the complementary framework for **operating and sustaining** those services once they are deployed. ITIL (Information Technology Infrastructure Library) provides internationally recognised best practices for IT service management, ensuring that digital services remain available, secure, and continuously improving.

> **Integration with Blueprint Governance:**
>
> ITIL service operations integrate with the Cybersecurity & Resilience Pod (→ Blueprint Section 4.E) and support the national digital resilience plan described in Phase 3B. This framework ensures that services built according to Blueprint standards are operated professionally and sustainably.

### Core ITIL Service Management Processes

The following five ITIL processes form the operational foundation for all digital services:

### 1. Incident Management

**Objective:** Restore normal service operation as quickly as possible with minimal business impact

**Key Activities:**

- Incident detection and logging
- Incident categorisation and prioritisation
- Investigation and diagnosis
- Resolution and recovery
- Incident closure and user confirmation

**Priority Matrix:**

| Priority | Impact | Response Time | Resolution Target |
|---|---|---|---|
| **P1 - Critical** | National service down, data breach, security incident | 15 minutes | 4 hours |
| **P2 - High** | Major functionality unavailable, significant user impact | 1 hour | 8 hours |
| **P3 - Medium** | Minor functionality issues, workaround available | 4 hours | 2 business days |
| **P4 - Low** | Cosmetic issues, minimal user impact | 1 business day | 5 business days |

**Escalation Path:**

1. Ministry Technical Liaison (first response)
2. CDU Pod Technical Lead (if unresolved within target time)
3. AIRB (for cross-ministry or architectural issues)
4. Cybersecurity & Resilience Pod (for security incidents)
5. Steering Committee (for national impact incidents)

**Documentation Required:**

- Incident Log Entry (Template in Part 5.4)
- Resolution Documentation
- Post-Incident Review (for P1/P2 incidents)

### 2. Change Management (Change Enablement)

**Objective:** Ensure changes to services are assessed, approved, and implemented safely

**Key Activities:**

- Change request submission and logging
- Impact and risk assessment
- Change approval (based on risk level)
- Change implementation and testing
- Post-implementation review

**Change Categories:**

| Category | Description | Approval Authority | Lead Time |
|---|---|---|---|
| **Standard** | Pre-approved, low-risk, routine changes (e.g., content updates) | Ministry Technical Liaison | 1 business day |
| **Normal** | Medium-risk changes requiring assessment (e.g., feature additions) | CDU Pod Lead + AIRB review | 5-10 business days |
| **Emergency** | Urgent changes to fix critical issues (e.g., security patches) | Cybersecurity Pod + fast-track AIRB | As required (documented retrospectively) |

**Change Advisory Board (CAB):**

For Normal and Emergency changes, a Change Advisory Board will review and approve changes. The CAB consists of:

- AIRB representative (chair)
- Relevant CDU Pod lead(s)
- Ministry Technical Liaison (affected service)
- Cybersecurity & Resilience Pod representative

**Documentation Required:**

- Change Request Form (Template in Part 5.4)
- Impact Assessment
- Rollback Plan
- Post-Implementation Review

### 3. Problem Management

**Objective:** Identify and address root causes of recurring incidents

**Key Activities:**

- Problem identification from incident patterns
- Root cause analysis
- Known error documentation
- Permanent solution implementation
- Problem closure and lessons learned

**Trigger Criteria:**

- Three or more similar incidents within one month
- Any P1 incident (mandatory post-incident review)
- Recurring workarounds being used
- Trend analysis showing emerging issues

**Root Cause Analysis Method:**

Use the "5 Whys" technique or Fishbone Diagram to identify underlying causes:

1. Define the problem clearly
2. Ask "Why did this happen?" and document the answer
3. Repeat asking "Why?" for each answer until root cause is identified
4. Verify the root cause with evidence
5. Develop permanent solution addressing the root cause

**Documentation Required:**

- Problem Record
- Root Cause Analysis Report
- Known Error Database Entry
- Permanent Solution Implementation Plan

### 4. Service Continuity Management

**Objective:** Ensure critical services can be maintained or quickly restored during disruptions

**Key Activities:**

- Business impact analysis for each service
- Risk assessment and mitigation planning
- Continuity strategy development
- Disaster recovery planning and testing
- Regular continuity plan reviews and updates

**Service Classification:**

| Tier | Criticality | Maximum Tolerable Downtime | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
|---|---|---|---|---|
| **Tier 1 - Mission Critical** | National security, emergency services, essential citizen services | 1 hour | 30 minutes | 15 minutes |
| **Tier 2 - Business Critical** | High-impact services, significant user base | 4 hours | 2 hours | 1 hour |
| **Tier 3 - Important** | Supporting services, moderate impact | 24 hours | 8 hours | 4 hours |
| **Tier 4 - Standard** | Non-critical services, minimal immediate impact | 72 hours | 24 hours | 24 hours |

**Continuity Testing Schedule:**

- Tier 1 services: Quarterly disaster recovery drills
- Tier 2 services: Bi-annual testing
- Tier 3/4 services: Annual testing
- All tiers: Table-top exercises every 6 months

**Integration with Blueprint:**

Service Continuity Management directly supports the National Digital Resilience Plan (→ Blueprint Phase 3B) and coordinates with the Cybersecurity & Resilience Pod.

### 5. Service Level Management

**Objective:** Define, monitor, and report on agreed service levels

**Key Activities:**

- Service Level Agreement (SLA) definition and negotiation
- Continuous service level monitoring
- Regular reporting to stakeholders
- Service improvement planning
- SLA review and revision

**Standard SLA Metrics:**

| Metric | Definition | Target (Tier 1) | Target (Tier 2) |
|---|---|---|---|
| **Availability** | Percentage of time service is accessible | 99.9% (8.76 hours downtime/year) | 99.5% (43.8 hours downtime/year) |
| **Performance** | Average page load time | < 2 seconds | < 3 seconds |
| **Incident Response** | Time to first response for P1 incidents | < 15 minutes | < 30 minutes |
| **Incident Resolution** | Time to resolve P1 incidents | < 4 hours | < 8 hours |
| **User Satisfaction** | Service satisfaction score (1-5 scale) | > 4.0 | > 3.5 |

**Reporting Cadence:**

- Real-time dashboards for technical teams
- Weekly operational reports to Ministry Technical Liaisons
- Monthly service performance reports to CDU and AIRB
- Quarterly strategic reports to Steering Committee

## Operational Runbooks

Every deployed service must have a comprehensive operational runbook that includes:

- ☐ Service description and architecture overview
- ☐ Normal operating procedures and daily checks
- ☐ Incident response procedures (by incident type)
- ☐ Escalation contacts and procedures

- [ ] Known issues and workarounds
- [ ] Backup and recovery procedures
- [ ] Performance monitoring and alerting configuration
- [ ] Change management procedures specific to the service
- [ ] Security incident response procedures
- [ ] Disaster recovery procedures

**Template:** Operational Runbook Template provided in Part 5.4

## Integration with AI Model Lifecycle Management

For AI-powered services deployed using CRISP-DM (Part 2.1), additional ITIL considerations apply:

### AI-Specific Incident Types

- **Model Performance Degradation:** Accuracy/precision drops below acceptable thresholds
- **Model Drift:** Input data distribution changes significantly from training data
- **Bias Detection:** Fairness metrics indicate discriminatory outcomes
- **Explainability Failure:** Model unable to provide required explanations
- **Data Quality Issues:** Input data quality degrades affecting predictions

### AI Model Monitoring (Continuous - Per NIST AI RMF "Manage" Phase)

- Prediction accuracy tracking (daily)
- Model confidence distribution analysis (weekly)
- Input data drift detection (weekly)
- Fairness metric monitoring (monthly)
- Model retraining trigger assessment (monthly)

### AI Model Change Management

Model retraining and redeployment follow the Normal Change process with additional requirements:

- A/B testing in production (shadow mode)
- Explainability verification for new model version
- Bias testing with updated data
- AI Oversight Committee approval for production deployment
- Model registry update with new version metadata

# 2.3 Accessibility Compliance: WCAG 2.2 Implementation

*→ Operationalises the accessibility commitments in Blueprint Section 2 (UK GDS Service Standard) and supports the Service Design & UX Pod responsibilities in Blueprint Section 4.D.*

## Purpose and Context

The Digital Transformation Blueprint establishes user-centricity as a core principle through the OECD Digital Government Framework and UK GDS Service Standard. Universal accessibility is fundamental to this commitment — digital services must be usable by all citizens regardless of ability, device, or connectivity.

This section provides the specific technical standard and implementation guidance for ensuring all digital services meet international accessibility requirements.

> **Integration with Blueprint Governance:**
>
> WCAG 2.2 AA serves as the mandatory accessibility baseline for all services developed under the Blueprint. The Service Design & UX Pod (→ Blueprint Section 4.D) leads compliance verification, with ministry teams accountable for applying accessible design practices throughout delivery.

## WCAG 2.2 Level AA as Baseline Standard

**What is WCAG 2.2?**

Web Content Accessibility Guidelines (WCAG) 2.2, published by the World Wide Web Consortium (W3C), is the international standard for web accessibility. Level AA represents the recommended compliance level for government services globally.

**Why WCAG 2.2 AA?**

- **International Standard:** Adopted by governments worldwide including UK, EU, Australia, Canada
- **Legal Compliance:** Aligns with international accessibility laws and conventions
- **Inclusive by Design:** Benefits all users, not just those with disabilities
- **Mobile-Friendly:** Includes criteria for touch and mobile experiences
- **Future-Proof:** Most recent version (2023) with enhanced mobile and low-vision support

## The Four WCAG Principles (POUR)

### 1. Perceivable

Information and user interface components must be presentable to users in ways they can perceive.

**Key Requirements:**

- **Text Alternatives:** Provide alt text for all images, icons, and non-text content
- **Multimedia:** Provide captions for videos, transcripts for audio
- **Adaptable Content:** Content can be presented in different ways without losing information
- **Distinguishable:** Make it easy to see and hear content (colour contrast, text size, audio clarity)

**Common Issues to Avoid:**

- Images without alt text or with generic alt text ("image", "picture")
- Insufficient colour contrast (less than 4.5:1 for normal text, 3:1 for large text)
- Information conveyed by colour alone
- Text embedded in images
- Videos without captions or transcripts

### 2. Operable

User interface components and navigation must be operable by all users.

**Key Requirements:**

- **Keyboard Accessible:** All functionality available via keyboard (no mouse required)
- **Enough Time:** Users have sufficient time to read and interact with content
- **Seizure Prevention:** No content that flashes more than 3 times per second
- **Navigable:** Clear navigation, logical tab order, descriptive page titles
- **Input Modalities:** Support for pointer, touch, and voice input

**Common Issues to Avoid:**

- Keyboard traps (user can't navigate away using keyboard)
- Insufficient time limits without ability to extend
- Illogical or confusing tab order
- Links and buttons without clear purpose
- Auto-playing content without user control

### 3. Understandable

Information and operation of user interface must be understandable.

**Key Requirements:**

- **Readable:** Text content is readable and understandable (language declared, jargon explained)
- **Predictable:** Pages appear and operate in predictable ways
- **Input Assistance:** Help users avoid and correct mistakes (clear labels, error messages, validation)

**Common Issues to Avoid:**

- Complex language without explanations or summaries
- Inconsistent navigation across pages
- Forms without clear labels or instructions
- Error messages that don't explain how to fix the problem
- Unexpected context changes without warning

### 4. Robust

Content must be robust enough to be interpreted by a wide variety of user agents, including assistive technologies.

**Key Requirements:**

- **Compatible:** Maximize compatibility with current and future user tools
- **Valid Markup:** Use valid HTML and ARIA attributes correctly
- **Name, Role, Value:** All UI components have accessible names and roles

**Common Issues to Avoid:**

- Invalid HTML that breaks assistive technologies
- Incorrect or missing ARIA attributes
- Custom controls without proper accessibility implementation
- Dynamic content updates not announced to screen readers

## Accessibility Testing Protocol

Accessibility testing must be integrated at every stage of the service design and delivery process:

### Phase 1: Discovery & Alpha (Blueprint Phase 1D - Quick Win Pilots)

- ☐ Include users with disabilities in user research
- ☐ Test prototypes with keyboard-only navigation
- ☐ Verify colour contrast in initial designs
- ☐ Review content for plain language and readability

### Phase 2: Beta Development (Blueprint Phase 2 - Pilots & Platform Development)

- ☐ Automated accessibility scanning (use tools like axe, WAVE, or Lighthouse)
- ☐ Manual keyboard navigation testing (all interactive elements)
- ☐ Screen reader testing (NVDA, JAWS, or VoiceOver)
- ☐ Colour contrast verification for all text and UI elements
- ☐ Form validation and error message testing
- ☐ Mobile touch target size verification (minimum 44x44 pixels)
- ☐ Zoom testing (up to 200% without horizontal scrolling)

### Phase 3: Pre-Launch (Blueprint Phase 2 - Evaluation in CRISP-DM)

- ☐ Comprehensive manual accessibility audit by Service Design & UX Pod
- ☐ User acceptance testing with citizens who use assistive technologies
- ☐ Cross-browser and cross-device testing
- ☐ WCAG 2.2 AA compliance verification (all criteria)
- ☐ Accessibility statement preparation
- ☐ Documentation of any known issues with remediation plans

### Phase 4: Post-Launch (Blueprint Phase 3 - Institutionalisation)

- ☐ Ongoing automated monitoring for accessibility regressions
- ☐ User feedback mechanism for accessibility issues
- ☐ Regular accessibility audits (minimum annually)
- ☐ Accessibility training for content editors and administrators

## Accessibility Testing Checklist

Use this comprehensive checklist to verify WCAG 2.2 AA compliance:

### Visual Design

- ☐ Text contrast ratio at least 4.5:1 for normal text (3:1 for large text 18pt+)
- ☐ UI component contrast ratio at least 3:1 (buttons, form fields, icons)
- ☐ Information not conveyed by colour alone
- ☐ Text can be resized to 200% without loss of content or functionality
- ☐ Text spacing can be adjusted without breaking layout
- ☐ Focus indicators clearly visible (at least 3:1 contrast against background)

### Keyboard Navigation

- ☐ All interactive elements keyboard accessible (Tab, Enter, Space, Arrow keys)
- ☐ Logical tab order (follows visual flow)
- ☐ No keyboard traps
- ☐ Skip links provided to bypass repetitive content
- ☐ Focus visible at all times
- ☐ Shortcuts don't conflict with assistive technology shortcuts

### Content & Structure

- ☐ Page has descriptive and unique title
- ☐ Headings used correctly (H1 for page title, logical hierarchy)
- ☐ Landmarks used for major page regions (header, nav, main, footer)
- ☐ Lists used for list content (ul, ol, dl)
- ☐ Tables used only for tabular data (with proper headers)
- ☐ Language of page declared in HTML
- ☐ Changes in language marked inline

### Images & Media

- ☐ All images have appropriate alt text (or alt="" if decorative)
- ☐ Complex images have longer descriptions available
- ☐ Videos have captions
- ☐ Audio content has transcripts
- ☐ Media can be paused or stopped
- ☐ Auto-playing audio can be disabled within 3 seconds

### Forms & Interactive Elements

- ☐ All form fields have visible and programmatic labels
- ☐ Required fields clearly indicated
- ☐ Input purpose identified (autocomplete attributes for common fields)

- [ ] Error messages clear and associated with relevant fields
- [ ] Error prevention for critical actions (confirmation required)
- [ ] Sufficient time provided for form completion
- [ ] Submit buttons clearly labeled with action (not just "Submit")

#### Mobile & Touch

- [ ] Touch targets at least 44x44 pixels (or 24px with adequate spacing)
- [ ] Functionality available via both pointer and touch gestures
- [ ] No reliance on device motion (tilting, shaking) without alternatives
- [ ] Orientation not locked (unless essential)
- [ ] Content reflows properly on mobile viewports

## Accessibility Statement Template

Every digital service must publish an accessibility statement that includes:

#### Accessibility Statement for [Service Name]

**Compliance Status:** This service is [fully/partially/not] compliant with WCAG 2.2 Level AA.

**Date of Assessment:** [Date]

**Assessment Method:** This statement was prepared using a combination of automated tools and manual testing by the Service Design & UX Pod.

**Known Issues:**

- [List any known accessibility barriers with planned remediation dates]

**Feedback:** If you encounter accessibility barriers using this service, please contact [email/phone] and we will work to resolve the issue.

**Enforcement:** If you are not satisfied with our response, you may escalate to [relevant authority].

## Accessibility Training Requirements

All personnel involved in designing, building, or managing digital services must complete accessibility training:

| Role | Training Required | Frequency |
|---|---|---|
| Service Designers & UX Researchers | Comprehensive WCAG 2.2 training, inclusive design principles | Initial + annual refresher |
| Developers (Frontend) | Accessible HTML/CSS/JavaScript, ARIA, keyboard navigation | Initial + annual refresher |
| Content Editors | Accessible content creation (alt text, headings, plain language) | Initial + biennial refresher |
| QA Testers | Accessibility testing tools and methods | Initial + annual refresher |
| Procurement Officers | Accessibility requirements in vendor contracts | Initial + biennial refresher |

## 2.4 Data Governance Operations

*→ Operationalises the National Data Governance & Interoperability Standard described in Blueprint Phase 1B and supports the AI & Data Governance Pod responsibilities in Blueprint Section 4.B.*

### Purpose and Context

The Digital Transformation Blueprint establishes strategic data governance requirements through GovStack principles and X-Road interoperability standards. The National Data Governance & Interoperability Standard (→ Blueprint Phase 1B) sets the policy framework.

This section provides the operational procedures for implementing that framework day-to-day: how ministries classify data, how data sharing agreements are approved, how data quality is measured, and how metadata standards are applied.

### Data Classification Framework

All government data must be classified according to sensitivity and access requirements:

| Classification | Definition | Examples | Access Control |
|---|---|---|---|
| **Public** | Data intended for public release with no access restrictions | Published reports, public announcements, open datasets | No authentication required |
| **Internal** | Data for internal government use, not sensitive | Operational procedures, internal communications, administrative records | Authenticated government users |
| **Confidential** | Sensitive data requiring protection, unauthorised disclosure could cause harm | Personal data, financial records, draft policies, commercial-in-confidence | Role-based access, need-to-know basis, audit logging |
| **Restricted** | Highly sensitive data, unauthorised disclosure could cause serious harm | National security data, law enforcement intelligence, protected health information | Strict access controls, encryption at rest and in transit, comprehensive audit trails |

### Data Classification Procedure

Ministry Data Stewards lead the classification process:

1. **Inventory Data Assets:** Identify all data collections held by the ministry
2. **Assess Impact:** Evaluate potential harm from unauthorised disclosure, modification, or loss
3. **Apply Classification:** Assign classification level based on impact assessment
4. **Document:** Record classification in ministry data catalogue

5. **Review:** Re-assess classification annually or when data use changes

**Tool:** Data Classification Assessment Template provided in Part 5.2

### Data Quality Framework

Data quality is measured across six dimensions:

| Dimension | Definition | Measurement Method |
|---|---|---|
| **Accuracy** | Data correctly represents reality | Sample validation against authoritative sources |
| **Completeness** | All required data elements are present | Percentage of non-null values in required fields |
| **Consistency** | Data is uniform across systems and time | Cross-system reconciliation checks |
| **Timeliness** | Data is up-to-date and available when needed | Time lag between data creation and availability |
| **Validity** | Data conforms to defined formats and rules | Percentage of values passing validation rules |
| **Uniqueness** | No unintended duplication | Duplicate detection rate |

### Data Quality Scorecard

Ministries must maintain a data quality scorecard for each critical dataset:

| Dimension | Score (0-100) | Target | Status | Remediation Plan |
|---|---|---|---|---|
| Accuracy | [Score] | ≥ 95 | [Green/Amber/Red] | [Actions if below target] |
| Completeness | [Score] | ≥ 98 | [Status] | [Actions] |
| Consistency | [Score] | ≥ 95 | [Status] | [Actions] |
| Timeliness | [Score] | ≥ 90 | [Status] | [Actions] |
| Validity | [Score] | ≥ 99 | [Status] | [Actions] |
| Uniqueness | [Score] | ≥ 99 | [Status] | [Actions] |

**Overall Quality Rating:** [Excellent / Good / Fair / Poor]

**Fit for Purpose Assessment:** [Yes / With Limitations / No]

## Data Sharing Agreements

When data is shared between ministries or with external parties, a formal Data Sharing Agreement (DSA) is required:

### DSA Approval Process

1. **Request Submission:** Requesting ministry submits DSA request to data owner
2. **Impact Assessment:** Data owner conducts privacy and security impact assessment
3. **Technical Review:** CDU AI & Data Governance Pod reviews technical controls
4. **Legal Review:** Legal counsel reviews compliance with data protection laws
5. **AIRB Approval:** AIRB approves DSA if all reviews satisfactory
6. **Implementation:** Technical integration via secure interoperability layer (X-Road)
7. **Monitoring:** Ongoing audit logging and compliance monitoring

### DSA Key Components

Every Data Sharing Agreement must include:

- ☐ Purpose of data sharing (specific use cases)
- ☐ Legal basis for sharing
- ☐ Data elements to be shared (specific fields)
- ☐ Data classification level
- ☐ Access controls and authentication requirements
- ☐ Usage restrictions (what data can/cannot be used for)
- ☐ Data retention and deletion requirements
- ☐ Security and privacy safeguards
- ☐ Audit and monitoring requirements
- ☐ Breach notification procedures
- ☐ Agreement duration and renewal process
- ☐ Termination conditions

**Template:** Data Sharing Agreement Template provided in Part 5.2

## Metadata Standards

All datasets must be documented using standardised metadata following the Dublin Core Metadata Element Set enhanced with government-specific elements:

| Metadata Element | Description | Required? |
|---|---|---|
| **Title** | Name of the dataset | Yes |
| **Description** | Clear explanation of dataset content and purpose | Yes |
| **Publisher** | Ministry or agency responsible for the dataset | Yes |
| **Creator** | Entity that originally created the data | Yes |
| **Date Created** | When the dataset was first created | Yes |
| **Date Modified** | Last modification date | Yes |
| **Update Frequency** | How often the data is updated (real-time, daily, monthly, etc.) | Yes |
| **Coverage** | Geographic, temporal, or topical scope | Yes |
| **Format** | File format(s) available (CSV, JSON, XML, etc.) | Yes |
| **Classification** | Data classification level (Public, Internal, Confidential, Restricted) | Yes |
| **Quality Score** | Overall data quality rating | Yes (for critical datasets) |
| **Contact Point** | Ministry Data Steward or responsible officer | Yes |
| **Access Rights** | Who can access this data and how | Yes |
| **License** | Usage license (for public datasets) | If public |
| **Related Datasets** | Links to related or dependent datasets | If applicable |

### National Data Catalogue

The CDU AI & Data Governance Pod will maintain a central National Data Catalogue containing metadata for all government datasets. This catalogue:

- Enables data discovery across ministries
- Prevents duplication of data collection efforts
- Supports AI use case identification (data availability assessment)
- Facilitates compliance with transparency and open data commitments
- Provides foundation for data lineage tracking

Ministries are responsible for registering their datasets and keeping metadata current.

# Part 3: Capability Development System

*This section operationalises the Capability Building & Standards Adoption activities described in Blueprint Phase 2C and establishes the measurement framework for sustainable knowledge transfer.*

## 3.1 Multi-Layered Learning Model

### Purpose and Context

The Digital Transformation Blueprint identifies capability building as essential for sustainable transformation (→ Blueprint Phase 2C). Training is described as an activity covering service design, AI governance, data management, cybersecurity, and interoperability.

This section provides the detailed delivery model for how that training will be structured, delivered, and sustained. The approach moves beyond traditional classroom training to embed learning within actual delivery work.

> **Core Principle:**
>
> Build internal capability, not dependency. Every pilot implementation is also a capability-building opportunity where ministry staff learn by doing alongside experts.

### The Four Learning Layers

Capability development uses a blended approach with four complementary layers:

### Layer 1: Structured Workshops

**Purpose:** Provide foundational knowledge and conceptual understanding

**Format:**

- 2-4 hour sessions delivered by CDU pods or external experts
- Mix of presentation, discussion, and hands-on exercises
- Maximum 20 participants per session for interactivity
- Materials provided for self-study and reference

**Topics Covered:**

- AI fundamentals and governance principles
- Data governance and quality management
- Service design and user research methods
- Digital accessibility (WCAG 2.2)
- Cybersecurity awareness and resilience
- Interoperability and API basics
- Agile delivery methods

**Delivery Schedule:** Foundational workshops delivered in Phase 1 (Months 0-3), with ongoing topic-specific sessions throughout implementation

### Layer 2: On-the-Job Mentoring

**Purpose:** Apply knowledge in real delivery contexts with expert guidance

**Format:**

- One-on-one or small group mentoring during pilot implementation
- Expert works alongside ministry staff on actual tasks
- Focus on problem-solving real challenges as they arise
- Structured reflection and learning documentation

**Mentoring Activities:**

- Co-development of use case definitions
- Joint data quality assessment
- Paired user research and testing
- Collaborative model evaluation
- Joint troubleshooting of technical issues

**Time Commitment:** Minimum 4 hours per week per mentee throughout pilot implementation (Phases 2-3)

### Layer 3: Shadowing & Pair Working

**Purpose:** Build practical skills through observation and active participation

**Format:**

- **Shadowing:** Ministry staff observe expert performing tasks, with explanation of decisions and techniques
- **Pair Working:** Staff and expert work together on tasks, gradually shifting leadership to staff member
- Regular role reversal: expert observes staff and provides feedback

**Typical Activities:**

- Data preparation and cleaning
- API testing and integration
- Accessibility testing
- Dashboard configuration
- Documentation writing
- Stakeholder presentations

**Progression Model:**

1. **I do, you watch** (expert demonstrates)
2. **I do, you help** (staff assists expert)
3. **You do, I help** (staff leads with expert support)
4. **You do, I watch** (staff works independently with observation)

### Layer 4: Communities of Practice & Data Clinics

**Purpose:** Foster peer learning, problem-solving, and knowledge sharing across ministries

**Communities of Practice (CoPs):**

- Regular meetings (monthly) of practitioners working on similar challenges
- Share experiences, artefacts, and lessons learned
- Discuss common problems and solutions
- Build professional networks across government

**Proposed CoPs:**

- AI & Data Analytics Practitioners
- Service Designers & UX Researchers
- Digital Architecture & Integration Specialists
- Accessibility Champions
- Agile Delivery Managers

**Data Clinics:**

- Bi-weekly drop-in sessions where staff can bring specific data challenges
- Expert facilitation from CDU AI & Data Governance Pod
- Hands-on problem-solving in safe learning environment
- Focus on practical skills: data interpretation, quality assessment, visualization

## Training Curriculum Overview

The following table shows the structured training programme aligned to the 12-month roadmap:

| Phase | Training Focus | Target Audience | Delivery Method |
|---|---|---|---|
| **Phase 1 (Months 0-3)** | • Digital government fundamentals<br>• AI & data governance principles<br>• Service design basics<br>• Accessibility awareness | All DFPs, Ministry Data Stewards, Ministry Technical Liaisons | Structured workshops + reading materials |
| **Phase 2 (Months 4-8)** | • CRISP-DM methodology<br>• Data quality assessment<br>• User research methods<br>• API integration basics<br>• WCAG 2.2 testing | Pilot project team members | Workshops + on-the-job mentoring + pair working |
| **Phase 3 (Months 9-12)** | • ITIL service operations<br>• AI model monitoring<br>• Advanced accessibility<br>• Train-the-trainer programme | Operational staff + identified internal champions | Mentoring + shadowing + train-the-trainer |

### Time Commitment Requirements

Ministry counterparts must allocate sufficient time for meaningful capability development:

| Role | Structured Training | On-the-Job Learning | CoP/Clinics | Total Time |
|---|---|---|---|---|
| **Ministry Digital Focal Point** | 5 days over 12 months | 4 hours/week during pilots | 2 hours/month | ~10-15% of time |
| **Ministry Data Steward** | 7 days over 12 months | 6 hours/week during pilots | 4 hours/month | ~15-20% of time |
| **Ministry Technical Liaison** | 10 days over 12 months | 8 hours/week during pilots | 4 hours/month | ~20-25% of time |

**Note:** This time investment is essential for building sustainable capability. Ministries must factor this into resource planning and secure management commitment.

## 3.2 Kirkpatrick Evaluation Framework

### Purpose and Context

Training effectiveness must be measured to ensure capability building delivers tangible value. The Kirkpatrick Four-Level Model provides a structured approach to evaluating training from participant reaction through to organizational results.

This framework ensures that capacity building efforts translate into practical competency within ministries and measurable improvements in digital transformation delivery.

### The Four Kirkpatrick Levels

#### Level 1: Reaction

**Question:** Did participants find the training valuable and relevant?

**Measurement Method:**

- Post-training evaluation surveys (immediately after each session)
- 5-point Likert scale questions
- Open-ended feedback

**Key Questions:**

- ☐ Was the training relevant to your role?
- ☐ Was the content clear and well-organized?
- ☐ Was the facilitator knowledgeable and engaging?
- ☐ Were the materials useful?
- ☐ Would you recommend this training to colleagues?

**Success Target:** Average satisfaction score ≥ 4.0 out of 5.0

**Action if Below Target:** Review training content, delivery method, and facilitator effectiveness; adjust for subsequent sessions

### Level 2: Learning

**Question:** Did participants acquire the intended knowledge and skills?

**Measurement Method:**

- Pre-training and post-training assessments
- Practical exercises and quizzes
- Competency demonstrations

**Assessment Types:**

- **Knowledge Tests:** Multiple choice or short answer questions on key concepts
- **Practical Assessments:** Hands-on tasks (e.g., conduct data quality assessment, write accessibility test case)
- **Case Study Analysis:** Apply learning to realistic scenarios

**Success Target:** 80% of participants demonstrate competency (pass practical assessment)

**Action if Below Target:** Provide remedial training or additional mentoring for individuals; identify common knowledge gaps for curriculum improvement

### Level 3: Behavior

**Question:** Are participants applying their learning in their work?

**Measurement Method:**

- On-the-job observation by mentors/supervisors (30-90 days post-training)
- Review of work artifacts produced by trainees
- Self-assessment surveys
- Peer feedback

**Observable Behaviors:**

- ☐ Conducting proper data quality assessments before analysis
- ☐ Following CRISP-DM methodology in AI pilots
- ☐ Applying accessibility testing protocols
- ☐ Using correct terminology and concepts in discussions
- ☐ Seeking guidance appropriately (not dependent, but appropriately asking questions)
- ☐ Sharing learning with colleagues

**Success Target:** 70% of participants consistently applying learned skills within 90 days

**Action if Below Target:** Investigate barriers (lack of management support, insufficient practice opportunities, unclear expectations); provide additional coaching; adjust workplace support structures

### Level 4: Results

**Question:** Did the training contribute to organizational objectives?

**Measurement Method:**

- Track key performance indicators before and after training
- Analyze pilot project outcomes
- Measure efficiency gains
- Assess quality improvements

**Key Result Metrics:**

| Metric | Baseline | Target Improvement |
|---|---|---|
| Number of AI use cases identified by ministry staff | 0 (pre-training) | 5+ per ministry by Month 12 |
| Data quality scores for critical datasets | [Assessed in Phase 1] | 10-15% improvement by Month 12 |
| Accessibility compliance rate | [Assessed in Phase 1] | 100% of new services WCAG 2.2 AA compliant |
| Time to implement pilot projects | [First pilot baseline] | 20% reduction by third pilot |
| Post-deployment support requests | [Measure first pilot] | 30% reduction by Month 12 (due to better knowledge transfer) |
| Independent ministry-led initiatives | 0 | At least 2 ministries initiating own digital projects by Month 12 |

**Success Target:** Achieve 70% or more of targeted result improvements

**Action if Below Target:** Conduct comprehensive review of training programme, delivery approach, and organizational support; adjust strategy for subsequent phases

## Evaluation Schedule and Reporting

| Kirkpatrick Level | When Measured | Responsible Party | Reporting To |
|---|---|---|---|
| **Level 1: Reaction** | Immediately after each training session | Training facilitator | CDU Delivery Lead (monthly summary) |
| **Level 2: Learning** | End of training module | Training facilitator + assessors | CDU Delivery Lead + Ministry DFPs (monthly) |
| **Level 3: Behavior** | 30-90 days post-training | Mentors + Ministry supervisors | CDU + AIRB (quarterly) |
| **Level 4: Results** | 6 months and 12 months post-training | CDU Delivery Lead + Programme Analyst | Steering Committee (biannual) |

## 3.3 Knowledge Transfer Mechanisms

### Purpose and Context

Sustainable digital transformation requires that knowledge remains within government institutions even as external experts complete their assignments. This section defines the mechanisms for ensuring effective knowledge transfer and institutional memory.

### Knowledge Transfer Plan Template

Every pilot implementation must include a documented Knowledge Transfer Plan with the following components:

### Knowledge Transfer Plan for [Pilot Name]

**1. Target Audience**

- Primary recipients: [Names, roles, ministry]
- Secondary audience: [Wider team, other ministries]

**2. Knowledge to be Transferred**

| Knowledge Area | Description | Priority |
|---|---|---|
| Technical Skills | [e.g., data preparation techniques, model evaluation methods] | High/Medium/Low |
| Process Knowledge | [e.g., CRISP-DM workflow, governance approval process] | High/Medium/Low |
| Domain Knowledge | [e.g., understanding of specific business context] | High/Medium/Low |
| Documentation | [e.g., system architecture, operational procedures] | High/Medium/Low |

**3. Transfer Activities**

| Activity | Method | Timeline | Responsible |
|---|---|---|---|
| [e.g., Data preparation training] | [e.g., Pair working + documentation] | [e.g., Weeks 4-8] | [Expert + Ministry staff] |

**4. Success Criteria**

- Ministry staff can perform [specific task] independently
- All documentation reviewed and approved by recipients
- Recipients pass practical competency assessment
- Ministry staff successfully troubleshoot common issues without external support

**5. Verification Method**

- Observed performance during handover period
- Practical assessment/demonstration
- Post-handover support metrics (should decrease over time)

## Documentation Standards for Knowledge Transfer

All pilots must produce the following documentation artifacts for knowledge retention:

| Document Type | Purpose | Minimum Content |
|---|---|---|
| **Project Overview** | High-level summary for stakeholders | Business objectives, approach, outcomes, lessons learned |
| **Technical Architecture** | System design reference | Component diagram, data flows, integration points, technology stack |
| **Operational Runbook** | Day-to-day operations guide | Procedures, monitoring, troubleshooting, contacts (see Part 2.2) |
| **User Guide** | End-user documentation | How to use the service, FAQs, support contact |
| **Data Documentation** | Data understanding | Data dictionary, quality assessment, sources, transformations |
| **Model Documentation (AI pilots)** | AI model transparency | Purpose, training data, features, performance metrics, limitations, monitoring |
| **Code Repository** | Technical implementation | Well-commented code, README, setup instructions, dependencies |
| **Lessons Learned** | Continuous improvement | What worked, what didn't, recommendations for future projects |

## National Knowledge Repository

The CDU will establish and maintain a centralized National Knowledge Repository accessible to all government personnel involved in digital transformation:

### Repository Structure

- **Standards & Frameworks:** All national standards, methodologies, and frameworks
- **Templates & Tools:** Reusable templates, checklists, and assessment tools
- **Project Documentation:** Complete documentation from all pilots and implementations
- **Training Materials:** Workshop presentations, guides, videos, reference materials
- **Reusable Code & Components:** Code libraries, APIs, common components
- **Case Studies:** Detailed write-ups of successful implementations
- **Communities of Practice:** Discussion forums, shared resources, member directories

### Repository Governance

- **Content Curation:** CDU Delivery Lead approves all published content
- **Quality Standards:** All documents must meet minimum quality standards (clear, complete, current)
- **Version Control:** All documents versioned and dated
- **Search & Discovery:** Proper tagging and metadata for easy findability

- **Access Control:** Role-based access (some content public, some government-only)
- **Regular Review:** Annual review to archive outdated content

## Train-the-Trainer Programme

In Phase 3 (Months 9-12), selected ministry staff will be trained to become internal trainers and coaches:

### Trainer Selection Criteria

- ☐ Successfully completed all relevant training (Kirkpatrick Level 2 pass)
- ☐ Demonstrated consistent application of skills (Kirkpatrick Level 3)
- ☐ Strong communication and interpersonal skills
- ☐ Respected by peers within their ministry
- ☐ Committed to supporting broader digital transformation
- ☐ Endorsement from Ministry Digital Focal Point

### Train-the-Trainer Curriculum

| Module | Duration | Content |
|---|---|---|
| **Adult Learning Principles** | Half day | How adults learn, learning styles, motivation |
| **Training Design** | 1 day | Needs assessment, learning objectives, content structuring |
| **Facilitation Skills** | 1 day | Presentation techniques, managing discussions, handling questions |
| **Assessment & Feedback** | Half day | Designing assessments, providing constructive feedback |
| **Mentoring & Coaching** | 1 day | One-on-one coaching techniques, building confidence |
| **Practice Teaching** | 2 days | Deliver sample training sessions, receive feedback, refine |

### Internal Trainer Responsibilities

Once certified, internal trainers will:

- Deliver foundational training to new staff in their ministry
- Provide ongoing coaching and mentoring to colleagues
- Facilitate ministry-level communities of practice
- Contribute content to the National Knowledge Repository
- Participate in national trainer community (coordinated by CDU)
- Maintain their own skills through continuous professional development

# Part 4: Delivery Governance & Collaboration

*This section operationalises the governance structures defined in Blueprint Sections 4 and 6, providing detailed responsibilities, decision-making protocols, and collaboration mechanisms.*

## 4.1 Expanded RACI Matrix

### Purpose and Context

The Digital Transformation Blueprint establishes a three-tier governance model with clear strategic, technical, and operational layers (→ Blueprint Section 6). This section provides detailed RACI (Responsible, Accountable, Consulted, Informed) matrices showing who does what for all major programme activities.

> **RACI Definitions:**
>
> - **Responsible (R):**
>
>  Person(s) who perform the work
> - **Accountable (A):**
>
>  Person who has final authority and accountability for the task (only one A per task)
> - **Consulted (C):**
>
>  People whose input is sought (two-way communication)
> - **Informed (I):**
>
>  People who are kept up-to-date (one-way communication)

## Programme-Level RACI

| Activity | Steering Committee | AIRB | AI Oversight Committee | CDU Delivery Lead | CDU Pods | Ministry DFPs |
|---|---|---|---|---|---|---|
| **National Digital Service Standard Development** | A | C | I | R | R | C |
| **National Data Governance Standard Development** | A | C | I | R | R (AI & Data Pod) | C |
| **AI Readiness Assessment (Ministry-Level)** | I | I | C | C | R (AI & Data Pod) | R, A |
| **Digital Building Blocks Development** | A (funding) | A (technical approval) | I | R | R (Architecture Pod) | C |
| **Pilot Project Selection** | A | C | C (if AI) | R | C | R (propose) |
| **Training Programme Development** | I | I | I | A | R | C |
| **Training Delivery** | I | I | I | A | R | R (attend) |
| **Knowledge Repository Management** | I | C | I | A | R | C (contribute) |
| **Cybersecurity Baseline Requirements** | A | A (technical approval) | I | C | R (Cyber Pod) | C |
| **Budget Allocation & Tracking** | A | I | I | R | C | I |
| **Monthly Progress Reporting** | I | I | I | R, A | R (contribute) | R (ministry updates) |

## Pilot Implementation RACI (Detailed)

For each ministry pilot following CRISP-DM methodology (Part 2.1):

| CRISP-DM Phase / Activity | AI Unit Expert | Ministry DFP | Ministry Data Steward | CDU AI Pod | AIRB | AI Oversight |
|---|---|---|---|---|---|---|
| **Phase 1: Business Understanding** | | | | | | |
| Use Case Definition | C | R, A | C | C | I | I |
| Success Metrics Definition | R | A | C | C | I | I |
| AI Risk Classification | R | C | C | A | I | I |
| **Phase 2: Data Understanding** | | | | | | |
| Data Access Provisioning | I | A | R | C | I | I |
| Data Quality Assessment | R | C | R | C | I | I |
| Privacy Impact Assessment | C | A | R | R | I | I |
| **Phase 3: Data Preparation** | | | | | | |
| Data Cleaning & Transformation | R | I | C (validation) | C | I | I |
| Bias Assessment | R | C | C | A | I | I |
| **Phase 4: Modeling** | | | | | | |
| Model Development | R | I | I | C | I | I |
| Model Performance Validation | R | C (business validation) | C | A | I | I |
| Explainability Documentation | R | C | I | A | I | I |
| **Phase 5: Evaluation** | | | | | | |
| User Acceptance Testing | C | R, A | R (participate) | C | I | I |
| Technical Assurance Review | C | I | I | R | A | I |
| Deployment Approval | I | C | I | C | C | A |
| **Phase 6: Deployment** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Production Deployment | R | A (accept) | C | C | I | I |
| Knowledge Transfer | R | R (receive), A | R (receive) | C | I | I |
| Operational Handover | R (deliver) | R (receive), A | C | C | I | I |

## Escalation Pathways

When issues cannot be resolved at the working level, clear escalation paths ensure timely decision-making:

### Issue Category 1: Technical Challenges

**Examples:** Integration difficulties, technical debt, performance issues, tool limitations

**Escalation Path:**

1. AI Unit Expert + Ministry Technical Liaison (attempt resolution)
2. Relevant CDU Pod Lead (within 3 business days if unresolved)
3. AIRB (if cross-ministry impact or architectural decision needed)
4. Steering Committee (if budget or strategic change required)

### Issue Category 2: Data Access or Quality

**Examples:** Data unavailable, poor quality, privacy concerns, data sharing disputes

**Escalation Path:**

1. Ministry Data Steward (attempt resolution within ministry)
2. CDU AI & Data Governance Pod (within 5 business days)
3. AIRB (if policy interpretation or cross-ministry data sharing)
4. Steering Committee (if requires ministerial intervention)

### Issue Category 3: Resource or Timeline

**Examples:** Ministry staff unavailable, delays, scope creep, budget overrun

**Escalation Path:**

1. Ministry DFP + CDU Delivery Lead (attempt mitigation)
2. Steering Committee (within 10 business days if significant impact)

### Issue Category 4: AI Risk or Ethics

**Examples:** Bias detected, fairness concerns, unexpected model behavior, ethical implications

**Escalation Path:**

1. CDU AI & Data Governance Pod (immediate assessment)
2. AI Oversight & Risk Governance Committee (within 2 business days)
3. Steering Committee (if requires deployment pause or policy change)

# 4.2 Ministry Counterpart Responsibilities

## Purpose and Context

The Blueprint defines ministry-level structures including Digital Focal Points, Data Stewards, and Technical Liaisons (→ Blueprint Section 4.2). This section details their specific responsibilities, expected deliverables, and success criteria.

> **Co-Delivery Principle:**
>
> Digital transformation is not something done TO ministries by external experts — it is done WITH ministries through active partnership. Ministry counterparts are not passive recipients but active participants in design, delivery, and ownership.

## Ministry Digital Focal Point (DFP)

### Primary Role

The DFP is the primary liaison between the ministry and MITCI's Central Digital Delivery Unit. They coordinate all digital transformation activities within their ministry and ensure alignment with both ministry objectives and national standards.

### Key Responsibilities

- ☐ Coordinate ministry participation in Blueprint implementation activities
- ☐ Identify and prioritize pilot project opportunities within the ministry
- ☐ Ensure ministry staff availability for training, pilots, and knowledge transfer
- ☐ Participate in monthly coordination meetings with CDU
- ☐ Report progress, challenges, and resource needs to ministry leadership
- ☐ Champion digital transformation within the ministry
- ☐ Facilitate access to ministry stakeholders, data, and systems
- ☐ Review and approve ministry-specific deliverables

### Expected Time Commitment

- **Phase 1 (Months 0-3):** 20% of time (1 day/week) — assessments, planning, training
- **Phase 2 (Months 4-8):** 30% of time (1.5 days/week) — active pilot involvement
- **Phase 3 (Months 9-12):** 15% of time — institutionalization, handover

### Key Deliverables

| Deliverable | Due | Description |
|---|---|---|
| Ministry Digital Readiness Assessment (input) | Month 2 | Complete assessment questionnaire, facilitate stakeholder interviews |
| Pilot Project Proposals | Month 3 | Identify 2-3 potential pilots with business case |
| Monthly Progress Reports | Ongoing | Update on pilot progress, resource issues, achievements |
| User Acceptance Sign-Off | Per pilot | Formal acceptance of completed pilot implementations |
| Knowledge Transfer Confirmation | Per pilot | Verify ministry staff competency post-handover |

### Success Criteria

- Ministry completes at least one pilot implementation by Month 8
- 90% attendance at required training and coordination meetings
- Timely provision of requested data, access, and resources
- Positive feedback from CDU on collaboration quality
- Ministry staff demonstrate competency in transferred knowledge

## Ministry Data Steward

### Primary Role

Ensure data governance, quality, classification, and compliance within the ministry. Act as the expert on ministry data assets and their appropriate use.

### Key Responsibilities

- ☐ Maintain ministry data catalogue and metadata
- ☐ Classify ministry data assets per national standards
- ☐ Conduct and document data quality assessments
- ☐ Facilitate data access for approved pilots and initiatives
- ☐ Ensure compliance with National Data Governance Standard
- ☐ Coordinate data sharing agreements with other ministries
- ☐ Participate in data-related training and data clinics
- ☐ Advise on data privacy and security considerations

### Expected Time Commitment

- **Phase 1:**

## 5.1 Service Design Templates

### Service Design Canvas

#### Service Design Canvas for [Service Name]

| | |
|---|---|
| **Service Vision:** [One sentence describing the service purpose and value] | |
| **User Needs**<br>[What users need to accomplish] | **User Pains**<br>[Current problems and frustrations] |
| **User Journey**<br>[Key steps users take] | **Touchpoints**<br>[Where users interact with government] |
| **Service Features**<br>[What the service will do] | **Success Metrics**<br>[How we measure success] |
| **Dependencies**<br>[What else is needed] | **Risks**<br>[What could go wrong] |

### User Research Protocol Template

#### User Research Plan for [Service Name]

**Research Objectives:**

- [What we want to learn]

**Research Methods:**

- ☐ User interviews
- ☐ Surveys
- ☐ Observation/shadowing
- ☐ Usability testing
- ☐ Focus groups

**Participant Criteria:**

- [Who we need to talk to]
- [Diversity considerations - age, ability, digital literacy, language]

**Research Questions:**

1. [Question 1]
2. [Question 2]

**Timeline & Resources:**

- Duration: [weeks]
- Number of participants: [X]
- Team members: [names]

## 5.2 AI & Data Templates

*Comprehensive AI and data templates including Use Case Definition, Data Readiness Assessment, Model Performance Report, and Operational Runbook are provided in full detail within the National Knowledge Repository. Key template structures are outlined below.*

## AI Use Case Definition - Key Sections

**Template includes:**

- Basic information (name, ministry, owner, date)
- Problem statement and proposed AI solution
- Expected benefits and success metrics
- AI risk classification (per EU AI Act)
- Data requirements and sources
- Stakeholder analysis
- Constraints, assumptions, and risks
- Approval signatures (Business Owner, CDU AI Pod, AIRB)

## Data Quality Scorecard - Measurement Dimensions

**Six quality dimensions assessed (1-5 scale):**

- Accuracy - data correctly represents reality
- Completeness - all required elements present
- Consistency - uniform across systems and time
- Timeliness - current and regularly updated
- Validity - conforms to defined formats and rules
- Uniqueness - no unintended duplication

**Overall readiness classification:**

Ready / Ready with Minor Remediation / Not Ready

## 5.3 Training & Knowledge Transfer Templates

### Training Evaluation Form (Kirkpatrick Level 1)

**Training Evaluation: [Training Name]**

**Your Name (Optional):** _____

**Date:** _____

Please rate the following on a scale of 1-5 (1=Strongly Disagree, 5=Strongly Agree):

- The training content was relevant to my role
- The training objectives were clearly explained
- The content was well-organized and easy to follow
- The facilitator was knowledgeable and engaging
- The training materials were useful
- I can apply what I learned in my work
- I would recommend this training to colleagues

**What was most valuable?** _____

**What could be improved?** _____

## 5.4 Governance Templates

### Change Request Form - Structure

**Essential components:**

- Change details (ID, service/system, requester, date, category)
- Description of change and reason
- Impact assessment (systems, users, downtime, risk level)
- Implementation plan (date, duration, steps, testing)
- Rollback plan
- Approval signatures (Manager, Technical Owner, CAB if applicable)

## Data Sharing Agreement - Key Clauses

**Mandatory provisions:**

- Purpose and legal basis for sharing
- Specific data elements and classification
- Transfer method and access controls
- Usage restrictions and prohibitions
- Retention, deletion, and security requirements
- Privacy safeguards and audit requirements
- Breach notification procedures
- Termination conditions

# Appendices

## Appendix A: CRISP-DM Detailed Process Guide

Full step-by-step procedures for all six CRISP-DM phases are maintained in the National Knowledge Repository. Key process flows are summarized below.

### CRISP-DM Phase Summary

**Phase 1: Business Understanding (2-3 weeks)**

**Key outputs:** Use case definition, success criteria, stakeholder map, project plan

**Governance checkpoint:** AIRB use case approval, AI risk classification

**Phase 2: Data Understanding (2-4 weeks)**

**Key outputs:** Data catalogue, quality assessment, exploratory analysis, privacy impact assessment

**Governance checkpoint:** Data classification, data sharing agreements

**Phase 3: Data Preparation (3-6 weeks)**

**Key outputs:** Cleaned datasets, feature engineering, bias assessment, version-controlled data

**Governance checkpoint:** Data lineage documentation, security review

**Phase 4: Modeling (4-8 weeks)**

**Key outputs:** Trained models, performance reports, explainability documentation, fairness assessment

**Governance checkpoint:** CDU AI Pod technical review, model performance validation

**Phase 5: Evaluation (2-4 weeks)**

**Key outputs:** UAT results, accessibility testing, security assessment, go/no-go recommendation

**Governance checkpoint:** AIRB technical assurance, AI Oversight Committee deployment approval

**Phase 6: Deployment (2-3 weeks + handover)**

**Key outputs:** Production system, user documentation, operational runbook, monitoring dashboards

**Governance checkpoint:** Steering Committee final approval, knowledge transfer completion

## Appendix B: ITIL Process Workflows

### Incident Management Process Flow

1. **Detection:** User reports OR monitoring alert → Log incident with unique ID
2. **Categorization:** Assign type and priority (P1-P4 based on impact/urgency)
3. **Initial Diagnosis:** First-line support attempts resolution using known solutions
4. **Escalation:** If unresolved within target time, escalate per priority matrix
5. **Investigation:** Specialist team diagnoses root cause
6. **Resolution:** Implement fix and verify service restored
7. **Closure:** Confirm with user, complete documentation, close ticket
8. **Post-Incident Review:** For P1/P2, conduct review within 5 days, create problem record if needed

### Change Management Process Flow

1. **Request Submission:** Complete change request form with full details
2. **Impact Assessment:** Evaluate risks, affected systems, required downtime
3. **Categorization:** Classify as Standard, Normal, or Emergency
4. **Approval:** Route per category (Standard=Technical Owner, Normal=CAB, Emergency=Fast-track)
5. **Scheduling:** Plan implementation during approved change window
6. **Implementation:** Execute change per plan, document steps
7. **Testing:** Verify change successful, no adverse impacts
8. **Review:** Post-implementation review, update runbooks if needed

## Appendix C: WCAG 2.2 Compliance Checklist

Comprehensive checklist of all WCAG 2.2 Level AA success criteria organized by POUR principles. Full checklist available in National Knowledge Repository.

### Quick Reference - Critical Checkpoints

#### Must-Have for All Services

- ☐ All images have meaningful alt text (or alt="" if decorative)
- ☐ Colour contrast minimum 4.5:1 for normal text, 3:1 for large text
- ☐ All functionality available via keyboard
- ☐ No keyboard traps
- ☐ Visible focus indicators (minimum 3:1 contrast)
- ☐ Logical tab order following visual flow
- ☐ Descriptive page titles and headings
- ☐ Form fields have visible and programmatic labels
- ☐ Error messages clear and associated with fields
- ☐ Touch targets minimum 44x44 pixels (or 24px with spacing)
- ☐ Content reflows without horizontal scrolling at 320px
- ☐ Text can be resized to 200% without breaking

## Appendix D: Kirkpatrick Measurement Instruments

### Four-Level Evaluation Summary

| Level | Question | Method | When | Target |
|---|---|---|---|---|
| **1: Reaction** | Did they like it? | Post-training surveys | Immediately after | ≥4.0/5.0 satisfaction |
| **2: Learning** | Did they learn? | Assessments, quizzes | End of training | 80% pass rate |
| **3: Behavior** | Do they apply it? | On-job observation | 30-90 days post | 70% applying skills |
| **4: Results** | Did it help organization? | KPI tracking | 6 & 12 months | 70% of targets met |

## Appendix E: Glossary of Terms

**AIRB:** Architecture & Interoperability Review Board

**CDU:** Central Digital Delivery Unit

**CRISP-DM:** Cross-Industry Standard Process for Data Mining

**DFP:** Ministry Digital Focal Point

**GovStack:** Framework for digital building blocks (UNDP/ITU)

**ITIL:** Information Technology Infrastructure Library

**Kirkpatrick:** Four-level training evaluation model

**NIST AI RMF:** AI Risk Management Framework

**RACI:** Responsible, Accountable, Consulted, Informed matrix

**RTO/RPO:** Recovery Time/Point Objective

**SLA:** Service Level Agreement

**UAT:** User Acceptance Testing

**WCAG:** Web Content Accessibility Guidelines

**X-Road:** Secure data exchange layer technology

# END OF DOCUMENT

This Implementation Playbook is designed to be used in conjunction with
**FAIR Guideline**

For questions, clarifications, or support in applying this playbook,
contact the AI Unit (AIU)
Ministry of Information Technology, Communication and Innovation

Document Version: 0.1
Last Updated: March 2026
CONFIDENTIAL - Government of Mauritius