

## PART 2

---

### REQUIREMENT SPECIFICATIONS

## Table of Contents

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>1. INTRODUCTION .....</b>                                      | <b>5</b>  |
| <b>2. OBJECTIVE .....</b>                                         | <b>5</b>  |
| 2.1. BUSINESS CONTEXT .....                                       | 5         |
| <b>3. SCOPE OF TENDER AND DELIVERABLES.....</b>                   | <b>5</b>  |
| 3.1. SCOPE OF TENDER .....                                        | 6         |
| 3.2. PROJECT SCHEDULE .....                                       | 8         |
| 3.3. SCOPE OF WORK.....                                           | 9         |
| 3.4. PROJECT REQUIREMENTS.....                                    | 10        |
| 3.5. PROJECT MANAGEMENT.....                                      | 11        |
| <b>4. FUNCTIONAL REQUIREMENTS .....</b>                           | <b>15</b> |
| 4.1. USER ROLES.....                                              | 15        |
| 4.2. GRANT FUND MANAGEMENT .....                                  | 17        |
| 4.3. FRONT PORTAL.....                                            | 19        |
| 4.4. GRANT ADMINISTRATION .....                                   | 22        |
| 4.5. VENDOR AND PURCHASE ORDER (PO) CREATION AND MANAGEMENT ..... | 25        |
| 4.6. INVOICE AND DISBURSEMENT .....                               | 25        |
| 4.7. FORMS AND DIGITAL LETTERS GENERATION AND SIGNATURE.....      | 25        |
| 4.8. PROJECT AND GRANT CLOSURE MANAGEMENT.....                    | 28        |
| 4.9. CANDIDATE ONBOARDING AND ENDORSEMENT .....                   | 30        |
| 4.10. STATEMENT OF GRANT CLAIM (SOGC).....                        | 31        |
| 4.11. WORKFLOW MANAGEMENT AND NOTIFICATIONS .....                 | 32        |
| 4.12. REASSIGNMENT AND CONFLICT OF INTEREST MANAGEMENT .....      | 36        |
| 4.13. WATCHLIST AND COMPLIANCE MANAGEMENT .....                   | 37        |
| 4.14. INTEGRATION WITH EXTERNAL SYSTEMS .....                     | 38        |
| 4.15. STANDARD REPORTS .....                                      | 40        |
| 4.16. AD-HOC REPORTING AND DATA EXPORT .....                      | 41        |
| 4.17. DASHBOARDS AND KPIS.....                                    | 42        |
| 4.18. BUSINESS RULES ENGINE.....                                  | 43        |
| 4.19. DATA MIGRATION FROM LEGACY SYSTEMS.....                     | 44        |
| 4.20. DATA RETENTION AND ARCHIVAL.....                            | 46        |

|           |                                                            |           |
|-----------|------------------------------------------------------------|-----------|
| 4.21.     | ARTIFICIAL INTELLIGENCE INTEGRATION .....                  | 46        |
| <b>5.</b> | <b>NON-FUNCTIONAL REQUIREMENTS .....</b>                   | <b>47</b> |
| 5.1.      | MAINTENANCE SERVICE AND OPERATION SUPPORT .....            | 47        |
| 5.2.      | PROBLEM MANAGEMENT .....                                   | 49        |
| 5.3.      | ESCALATION PROCESS .....                                   | 52        |
| 5.4.      | PROBLEM MANAGEMENT SYSTEM.....                             | 52        |
| 5.5.      | CHANGE REQUEST .....                                       | 53        |
| 5.6.      | SERVICE REQUEST .....                                      | 54        |
| 5.7.      | TRAINING AND KNOWLEDGE TRANSFER .....                      | 55        |
| 5.8.      | COMMUNICATION PLAN .....                                   | 56        |
| 5.9.      | QUALITY ASSURANCE .....                                    | 56        |
| 5.10.     | DOCUMENTATION.....                                         | 57        |
| 5.11.     | EXIT MANAGEMENT .....                                      | 57        |
| 5.12.     | QUALITY ASSURANCE AND MEASUREMENT.....                     | 58        |
| 5.13.     | PERFORMANCE MEASUREMENT .....                              | 59        |
| 5.14.     | AUDIT .....                                                | 59        |
| <b>6.</b> | <b>TECHNICAL REQUIREMENTS .....</b>                        | <b>61</b> |
| 6.1.      | OBJECTIVE .....                                            | 61        |
| 6.2.      | USER INTERFACE .....                                       | 61        |
| 6.3.      | SIGN IN .....                                              | 61        |
| 6.4.      | LOG OUT FOR NON-ACTIVE USERS .....                         | 61        |
| 6.5.      | APPLICATION DESIGN.....                                    | 61        |
| 6.6.      | GENERATIVE AI-BASED SUMMARY / RECOMMENDATION ENGINES ..... | 62        |
| 6.7.      | AUTHORISATION DESIGN GUIDELINES .....                      | 62        |
| 6.8.      | UP-TO-DATE TECHNOLOGY .....                                | 62        |
| 6.9.      | EASE OF OPERATION .....                                    | 63        |
| 6.10.     | SYSTEM INTERFACE .....                                     | 64        |
| 6.11.     | EXCEPTION HANDLING .....                                   | 64        |
| 6.12.     | APPLICATION AUDIT .....                                    | 65        |
| 6.13.     | SUBCONTRACTOR AND THIRD-PARTY COMPLIANCE .....             | 65        |
| 6.14.     | SYSTEM PERFORMANCE AND LOAD TESTING .....                  | 65        |
| 6.15.     | SYSTEM AVAILABILITY .....                                  | 65        |

|                                          |                                    |           |
|------------------------------------------|------------------------------------|-----------|
| 6.16.                                    | BACKUP AND DISASTER RECOVERY ..... | 66        |
| 6.17.                                    | TECHNICAL DOCUMENTATION .....      | 66        |
| 6.18.                                    | INFRASTRUCTURE.....                | 67        |
| 6.19.                                    | SECURITY MEASURES.....             | 68        |
| 6.20.                                    | CERTIFICATIONS.....                | 70        |
| <b>ANNEX A: PAYMENT MILESTONES .....</b> |                                    | <b>71</b> |

## CONTENTS

### 1. INTRODUCTION

Employment and Employability Institute Pte Ltd

e2i is a tripartite initiative of the National Trades Union Congress set up to support nationwide manpower and skills upgrading initiatives.

Please see [e2i.com.sg](http://e2i.com.sg) for more information on e2i.

### 2. OBJECTIVE

The Employment and Employability Institute Pte Ltd (e2i) is calling for a revamp of its existing grant management portal. The tender is for the build and implementation of a Grant Management System, with a maintenance contract period of five (5) years, comprising an initial three (3) years with an option to extend for one (1) year plus a further one (1) year, subject to e2i's requirements and approval.

#### 2.1. Business Context

The Grant Management System (GMS) is a platform designed to manage the complete lifecycle of workforce development grants, from initial application submission by companies through to final disbursement, project closure, audit, and grant recovery where applicable.

The System shall support the administration of multiple grant types and schemes, the definitions and parameters of which may evolve over time. Current grant types include:

- (a) Institutional Grants (IG)
- (b) Career Conversion Programmes (CCP) with multiple modalities including Place-and-Train, Train-and-Place, Job Redesign Reskilling, and Job-Redeployment
- (c) Training allowances and salary support programmes
- (d) The System shall be extensible to accommodate new grant types, schemes, and funding components as they are introduced by the e2i.

### 3. SCOPE OF TENDER AND DELIVERABLES

### 3.1. Scope of Tender

- 3.1.1. The purpose of this Invitation to Tender (ITT) is to invite Tenderers to submit a complete proposal to provide the following Services:
- 3.1.2. BASE SERVICES: The successful Tenderer shall supply, provide and deliver the following base services:
- (a) **Implementation Services:** develop, configure, customise, test, implement and deliver the System, provide training and fulfill other requirements to provide a fully operational System complying with the requirements as set out in Clauses 4, 5, and 6
  - (b) **Platform Supply:** A comprehensive Grant Management System platform capable of meeting all requirements specified in Clauses 4, 5, and 6.
  - (c) **Integration Services:** Design, build, test, and deploy all required integrations to:
    - (i) National and organisational authentication providers such as Singpass, Corppass, organisational SSO and trusted data services for company profile and individual data population
    - (ii) External onboarding, eligibility verification and compliance services (including but not limited to ACRA, SWDA, and similar statutory or regulatory systems)
    - (iii) Enterprise financial systems for purchase order creation, invoicing, and disbursement tracking
  - (d) **Migration Services:** Complete migration of existing systems and its legacy data into the new GMS, ensuring to fulfill its functions, historical traceability, audit compliance, and operational continuity.
- 3.1.3. The Tenderer shall offer to provide the following as part of the services:
- (a) **Change Requests:** provision of services for e2i-approved enhancements or changes to the System (“Change Requests”) during the contract period from Effective Date during system implementation and maintenance period, where such services may procure 200 man-days per maintenance year throughout the contract period for the relevant types of IT manpower, pursuant to Clause 32 (Claims for Extra Work) of the Conditions of Contract. Any unused CR man-days at the end of a maintenance year shall be carried forward to the subsequent maintenance year and remain available for utilisation within the contract period, subject to e2i’s approval and applicable contract terms. The Tenderer shall state the volume discount if available. The Contractor shall only bill for Change Requests completed and accepted by e2i.

- 3.1.4. Any Proposal to supply only parts of the above shall be considered incomplete and deemed invalid for the purposes of the Tender. This Tender is an outcome-based tender which the Tender documents describe the outcomes desired by e2i, and the Tenderer shall propose how its approach and solution may achieve such outcomes, and if awarded the Tender, provide the solution as accepted by e2i.
- 3.1.5. The Tenderer shall clearly indicate and explain in the Tender proposal if the solution proposed is already productized or is a bespoke solution specifically developed for e2i.
- 3.1.6. The Tenderer shall clearly explain in the Tender proposal the technical architecture and how to interface with the existing e2i IT systems as stipulated in Clause 6 (Technical Requirements).
- 3.1.7. All governance requirements for implementing of the System shall be clearly mentioned in the Tender proposal.
- 3.1.8. All licensing requirements shall be clearly mentioned in the Tender proposal. The Tenderer shall quote for licenses to support 350 users for the launch of the system. The Tenderer should also quote for additional blocks of 10 user licenses, up to a maximum of 500 licenses. The Tenderer shall state the volume discount if available. Licenses should be transferrable.
- 3.1.9. The Tenderer shall propose the infrastructure architecture design, hosting capacity and components required to support the overall implementation and performance of the System. In the event of non-compatibles or system degradation, the Contractor shall propose solution/s and shall be responsible for procuring and adding system resources to meet the System requirements at no additional cost to e2i if the system degradation is due to poor design or coding practices by the Contractor.
- 3.1.10. The Tenderer is advised that in exigency of requirements, e2i has the right to re-prioritise the deliverables in the project schedule. This will be done in consultation with the successful Tenderer.
- 3.1.11. The Tenderer shall propose the project organisation structure, team composition, man-days and/or man-month rates of the various types of IT manpower, and proven methodology for agile Application Development Services. The Tenderer shall clearly indicate if any offshore resources, including the development and support, in their proposal.
- 3.1.12. The Acceptance Tests of the System shall be carried out at e2i's site.
- 3.1.13. The Contractor shall provide System support and maintenance and problem management services, as more particularly described in Clause 5, upon the implementation of the System in Production Environment. These services should be provided without additional cost to e2i till end of Performance

Guarantee Period (PGP), which during this period the Contractor shall demonstrate that the System operates in accordance with the Requirement Specifications and the following PGP Requirements.

- 3.1.14. The Contractor shall provide a six (6) month PGP, commencing from the Production Go-Live Date. The first eight (8) weeks of the PGP shall constitute the Hypercare Period during which on-site enhanced support services shall be provided.
- 3.1.15. Hypercare Period means the initial period immediately following Production Go-Live during which the Contractor shall provide enhanced support, monitoring, incident management, issue resolution, user assistance, and operational stabilization services to ensure a smooth transition to business-as-usual operations.
- (a) The Hypercare Period shall commence on the Production Go-Live date and continue for a minimum of 8 weeks or until e2i formally confirms successful operational stabilization.
  - (b) The Hypercare Period shall be completed only upon e2i's written acceptance that:
    - (i) All Severity 1 and 2 incidents have been resolved;
    - (ii) The System has achieved the agreed service levels and operational stability
- 3.1.16. The PGP shall be deemed successfully completed only when:
- (a) the System has achieved the required Service Availability Levels throughout the PGP
  - (b) no Severity 1 (Critical) or Severity 2 (High) defects remain unresolved;
  - (c) all material contractual and functional requirements continue to operate satisfactorily in the Production Environment
  - (d) all required operational documentation and knowledge transfer activities have been completed and accepted by e2i
  - (e) Knowledge transfer activities have been completed to operations and support teams
  - (f) The System is ready for transition to normal maintenance and support operations

### 3.2. Project Schedule

- 3.2.1. The Contractor shall adhere to the project timeline stipulated below:

| No | Activities       | Date                                            |
|----|------------------|-------------------------------------------------|
| 1  | Project kick off | Within 1 week from date of Letter of Acceptance |



| No | Activities                                      | Date                                                                                       |
|----|-------------------------------------------------|--------------------------------------------------------------------------------------------|
| 2  | Implementation Plan for all 3.1.2 Base Services | Within 2 weeks from date of Letter of Acceptance. Refer to Annex A for required milestones |
| 3  | System go-live                                  | Within 9 months from date of Letter of Acceptance                                          |

3.2.2. The Tenderer may propose a project schedule where the milestones can be achieved earlier for development and implementation phase.

### 3.3. Scope of Work

3.3.1. The Contractor shall minimally cover the following activities for System implementation, and the Tenderer may propose any additional services and software deemed necessary to meet e2i's requirements according to Section 4, 5, and 6 (Requirements Specification) and the contractual terms in the Conditions of Contract:

- (a) Detailed Requirements Study of e2i's requirements, including user interface/user experience planning, and the development of wireframing and high-fidelity prototypes;
- (b) project management;
- (c) provide all installation, backup and recovery procedures for the System.
- (d) integration of the System with other e2i applications;
- (e) Acceptance Tests of the System which include functionality tests, system integration tests (SIT), and System Performance Tests;
- (f) System commissioning;
- (g) rectification and closure of all findings from System security audits conducted by e2i appointed vendor(s) and/or independent security auditor during the contract period;
- (h) user training; and
- (i) System maintenance support and documentation.

### 3.3.2. Functional Specifications

- (a) The Contractor shall conduct Detailed Requirement Study to verify, confirm and understand the business detailed process flow, business rules and data requirements of e2i for the System.

- (b) The Contractor shall prepare and provide the draft Functional Specifications which shall minimally cover the following, for e2i's approval:
  - (i) user interface and user experience flow;
  - (ii) wireframe and prototypes;
  - (iii) business process flow;
  - (iv) business and data validation rules;
  - (v) data requirements;
  - (vi) reports requirements; and
  - (vii) external system integration.
- (c) The Contractor shall configure the System in accordance to the application design, database design and security requirements specified in Clauses 5 and 6.
- (d) The Contractor shall be responsible for all system integration activities related to the proposed solution (these include integrating all hardware and software necessary for the System even if they are not purchased through the Contractor).
- (e) The Contractor shall work closely with e2i's IT support team and e2i's outsourced service provider (Third-Party Vendor) for service management and Integration application support.
- (f) The Contractor shall work with e2i's vendors, particularly where the System will be integrating with external systems maintained by these vendors, to facilitate seamless integration between the System and such external systems, understudy the interface specifications, at no additional cost.

### 3.4. Project Requirements

#### 3.4.1. Project Phases:

The Contractor shall implement and deliver the System in ONE (1) phase, with all the functionalities and requirements stated in Clauses 4, 5 and 6.

#### 3.4.2. Functional Requirements:

The Contractor shall ensure that the System complies with the functional requirements as set out in Clause 4.

#### 3.4.3. Non-Functional Requirements:

The Contractor shall ensure that the System complies with the non-functional requirements as set out in Clause 5.

#### 3.4.4. Project Technical Requirements and Security Requirements:

The Contractor shall ensure that the System complies with the technical and security requirements as set out in Clause 6.

### 3.5. Project Management

3.5.1. e2i shall appoint a person to supervise and liaise with the Tenderer for the purpose of the Contract and such person may designate others to assist him/her in such matters.

3.5.2. The Tenderer shall propose a suitably qualified project team, or equivalent roles, to lead and manage the key project teams and workstreams.

(a) Project Director/Manager

Provides overall delivery leadership, governance, and accountability to keep scope, schedule, cost, quality, risks, and stakeholders aligned with agreed outcomes.

Preferably  $\geq 10$  years' experience or more

(b) Solution/Technical Architect

Owns the end-to-end solution architecture, ensuring the design meets functional, technical, security, integration, scalability, and operational requirements.

Preferably  $\geq 10$  years' experience or more

(c) Development Lead

Leads system build and configuration, ensuring approved requirements and designs are implemented with quality, consistency, and deployment readiness.

Preferably  $\geq 10$  years' experience or more

(d) Data Migration Lead

Plans and controls secure, accurate, and complete data migration, with business validation, reconciliation, and go-live readiness.

Preferably  $\geq 5$  years' experience or more

- (e) **Business Analyst/Functional Lead**  
Defines and manages business and functional requirements, ensuring the solution reflects user needs, operating processes, controls, and acceptance criteria.  
  
Preferably  $\geq 5$  years' experience or more
- (f) **Security/Compliance Lead**  
Ensures the solution meets security, privacy, compliance, audit, and risk requirements across design, build, testing, and operations.  
  
Preferably  $\geq 5$  years' experience or more
- (g) **UX Designer**  
Ensures the solution is intuitive, accessible, efficient, and aligned with key user journeys across internal and external users.  
  
Preferably  $\geq 5$  years' experience or more
- (h) **Integration Lead**  
Leads secure and reliable interfaces across internal and external systems, ensuring data flow, monitoring, error handling, and reconciliation are well controlled.  
  
Preferably  $\geq 5$  years' experience or more
- (i) **Test/QA Lead**  
Owns test strategy and quality assurance, ensuring the solution is validated against requirements, standards, business processes, and release criteria.  
  
Preferably  $\geq 5$  years' experience or more
- (j) **Training/Change Lead**

Prepares users, administrators, and support teams for adoption through readiness planning, communications, training, and post-go-live reinforcement.

Preferably 5 years' experience or more

- (k) Service Delivery Manager
- Governs transition into steady-state service, ensuring service levels, support arrangements, responsibilities, reporting, and supplier obligations are clear and measurable.

Preferably  $\geq 10$  years' experience or more

- (l) Ops/Support/Maintenance Lead
- Owns post-go-live support and maintenance, ensuring the solution remains stable, secure, supportable, monitored, and continuously improved.

Preferably  $\geq 5$  years' experience or more

3.5.3. The Tenderer shall establish, implement, and maintain a project governance throughout the project lifecycle. The governance shall include the following components:

- (a) Steering / Project Governance. Provides senior oversight, clear decision rights, accountability, and stakeholder alignment to keep the project strategically aligned and effectively governed.
- (b) Project Status Cadence. Establishes a clear reporting rhythm to provide timely visibility of progress, risks, issues, and decisions at project and executive levels.
- (c) RAID Log (Risks, Assumptions, Issues, Dependencies). Provides a single view of key risks, assumptions, issues, and dependencies, with ownership and mitigation actions to support proactive delivery control.
- (d) Escalation Path. Records key project decisions, rationale, approvals, and impacts to ensure traceability, accountability, and stakeholder alignment.

- (e) Change Control. Controls changes to scope, requirements, design, schedule, and cost through formal assessment, approval, prioritisation, and baseline updates.
  - (f) Quality / Stage-Gate Reviews. Applies stage-gate checkpoints to confirm deliverable quality, readiness, and compliance before progressing to the next phase.
- 3.5.4. Please refer to Clauses 7.2, 7.3 and 7.4 of Part I, Section B, Conditions of Contract, for requirements for the Project Organisation, Implementation Plan and Monthly Progress Reports.
  - 3.5.5. The Tenderer shall provide information on the personnel and expertise required as set out in Clause 7.2 of the Part I, Section B, Conditions of Contract.
  - 3.5.6. At least 2 weeks prior to the start of each stage, the Contractor shall provide a detailed Implementation Plan for the scope of the work to be done in that stage. The detailed Implementation Plan should include the dates of major milestones, key activities and the Contractor's personnel's roles and responsibilities, the activities requiring e2i and/or third parties' involvement as well as their roles and responsibilities, dependencies of the activities, and the critical path. The detailed Implementation Plan should factor in sufficient time for the Contractor and e2i to review the documents before e2i approves them.
  - 3.5.7. The Contractor shall update the detailed Implementation Plan regularly to reflect actual completion dates and may propose revisions to the planned dates with no impact to the project deadlines stipulated by e2i. All such updates and proposed revisions to the detailed Implementation Plans shall be subject to e2i's written approval.

## 4. FUNCTIONAL REQUIREMENTS

### 4.1. User Roles

- 4.1.1. The System shall support multiple user groups, consisting of distinct roles, with access and configuration with accordance with the organisational needs and business rules, user roles are as listed but not limited to the ones presented in the table below:

| S/N | User Role                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Applicant                           | Applicant is the grantee applying for the grant.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 2   | Partnership Group Officer-In-Charge | <p>Partnership Group Officer-In-Charge is involved in the Application, Project Variation, and Claims Processing workflows.</p> <p>In addition, Partnership Group OIC will be granted rights for viewing and generation of report and dashboards.</p> <p>Note: Partnership Group OICs will be classified into sectors and sub-sectors, to be made as part of the role-based configuration.</p>                                                                                                           |
| 3   | Partnership Group Team Lead         | <p>Partnership Group Team Lead is involved in the Application, Project Variation and Claims Processing workflows for supporting or rejecting the submission from the group of Partnership Group OICs tagged to them. Partnership Group Team Leads are sector based and should only review the projects of their sector(s) from the respective Partnership Group OICs.</p> <p>In addition, Partnership Group Team Leads will be granted rights for viewing and generation of reports and dashboards.</p> |

| S/N | User Role                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4   | Partnership Group Deputy CEO (DyCEO)    | Partnership Group DyCEO is involved in the Application, Project Variation and Claims Processing workflows for supporting/ rejecting the submission from the Partnership Group Team Lead respectively.<br><br>In addition, Partnership Group DyCEO will be granted rights for viewing and generation of reports and dashboards.                                                                                                                                   |
| 5   | Grant Processing Team Officer-In-Charge | Grant Processing Team Officer-In-Charge is involved in the Application, Project Variation and Claims Processing workflows for the purpose of reviewing and checking of information submitted. The GPT OIC who first retrieves the project is the reviewer of the project. After reviewing, the next GPT OIC who retrieves the project is the checker of the project. GPT Officer-In-Charge is non-sector based and is able to process projects from all sectors. |
| 6   | Grant Processing Team Team Lead         | Grant Processing Team Team Lead is involved in the support and decision making for Application, Project Variation and Claims Processing workflows based on authorised amounts. GPT Team Lead is non-sector based and is able to process projects from all sectors.                                                                                                                                                                                               |
| 7   | CGMG DyCEO                              | CGMG DyCEO is involved in the support and decision making for Application, Project Variation and Claims Processing workflows based on authorised amounts.                                                                                                                                                                                                                                                                                                        |
| 8   | CEO                                     | CEO is involved in the support and decision making for Application, Project Variation and Claims Processing workflows based on authorised amounts.                                                                                                                                                                                                                                                                                                               |
| 9   | Finance Officer-In-Charge               | Finance OIC have access to fund and grant management with the capability to administer and update the fund pots for Fund and Grants. Additionally Finance OIC will be granted access to claw back, reports, and dashboard module.                                                                                                                                                                                                                                |
| 10  | Finance Team Lead                       | The Finance Team Lead will have the authority to approve requests to update fund pots submitted by Finance Staff.                                                                                                                                                                                                                                                                                                                                                |
| 11  | Grant Policy Team Member                | The Grant Policy team member will have scheme management access, which includes but is not limited to,                                                                                                                                                                                                                                                                                                                                                           |



| S/N | User Role                                  | Description                                                                                                                                                                                                                                                             |
|-----|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                            | creation and update of schemes in Fund Management. In addition, Grant policy team members shall be granted rights to view projects and reports, including extraction/download of supporting documents and reports.                                                      |
| 12  | Grant Policy Team Lead                     | The Grant Policy team lead has approving rights for the creation and update of schemes in Fund Management. In addition, Grant policy team lead shall be granted rights to view projects and reports, including extraction/download of supporting documents and reports. |
| 13  | Governance, Risk, and Compliance Member    | The Governance, Risk and Compliance member will have viewing rights, report generation for audit, manage company watchlist, and put up audit (SOGC) requests.                                                                                                           |
| 14  | Governance, Risk, and Compliance Team Lead | The Governance, Risk and Compliance team lead will have the right to approve audit requests.                                                                                                                                                                            |
| 15  | Secretariat Office Member                  | Secretariat office members will be granted viewing rights to view projects, extract supporting documents and generate reports and dashboards.                                                                                                                           |
| 16  | PSDA Officer-in-Charge                     | PSDA OIC will be granted viewing rights to view projects, extract supporting documents and generate reports and dashboards.                                                                                                                                             |
| 17  | System Admin                               | System Admin has access to all available functions in GMS, except processing-related functions.                                                                                                                                                                         |

#### 4.2. Grant Fund Management

- 4.2.1. The System shall support a configurable, hierarchical fund structure, allowing the e2i to define multiple levels of funds, grants, schemes, and sub-schemes.
- 4.2.2. The System shall enable authorised users to create, modify, close, and archive fund entities (tranches, grants, schemes) with defined attributes including but not limited to:
  - (a) Start and end dates
  - (b) Allocated fund amounts
  - (c) Descriptions and metadata
  - (d) Approval workflows and approving authorities

- (e) Audit the compliance of the transactions on the system
- 4.2.3. The System shall support the definition of fund parameters at each level of the hierarchy, with inheritance and override capabilities (e.g., scheme-level parameters overriding grant-level defaults).
- 4.2.4. The System shall automatically manage unallocated fund balances at each level of the hierarchy, enabling transparent tracking of available funds.
- 4.2.5. The System shall support fund transfers and reallocation between schemes, grants, or other fund entities, subject to configurable approval workflows, scheduler for fund automated balance transfers, and locking rules.
- 4.2.6. The System shall support the creation and management of scheme parameters, including configurable funding components (such as course fees, salary support, training allowances, in-house training, and other funding types defined by the e2i).
- 4.2.7. The System shall allow funding components, caps, percentages, and eligibility rules to be configured per scheme without code changes.
- 4.2.8. Fund Management Dashboard and Tracking. The System shall provide a real-time Fund Management Dashboard accessible to authorised users, displaying configurable metrics including but not limited to:
  - (a) Fund entity names, total allocations, and unallocated balances
  - (b) Committed funding amounts (approved and locked)
  - (c) Uncommitted or pipeline funding amounts (applications in processing)
  - (d) Disbursed amounts
  - (e) Returned or recovered amounts
  - (f) Calculated balances and forecasts of fund utilization
- 4.2.9. The System shall automatically update fund balances in real-time or near-real-time based on transaction events including but not limited to application submissions, approvals, rejections, withdrawals, terminations, endorsements, project closures, project variations, and claim disbursements.
- 4.2.10. The System shall track and distinguish between different funding states (e.g., available, committed, conditionally committed, disbursed, returned) to support accurate fund availability calculations.
- 4.2.11. The System shall maintain a complete audit trail of all fund management transactions, including but not limited to creation, transfer, allocation, commitment, disbursement, and return activities, with timestamps, user attribution, and justifications.
- 4.2.12. The System shall support configurable alerts and notifications when fund balances fall below defined thresholds or when funding limits are approached.

#### 4.3. Front Portal

- 4.3.1. The System shall maintain a Company Profile module storing company information including unique entity number, company name, organisational classification, and other relevant attributes.
- 4.3.2. Upon authentication via corporate identity systems, the System shall synchronise company profile data with trusted external data sources, while retaining historical company data in the backend for audit, reference, and trend analysis.
- 4.3.3. The System shall perform eligibility checks using a combination of methods including:
  - (a) Self-declaration by the applicant or officer
  - (b) Real-time verification via API integration with statutory or regulatory systems (including but not limited to corporate registry, blacklist, de-blacklisting and compliance databases)
- 4.3.4. The System shall support configuration of eligibility rules, validation logic, and data locking policies to prevent unauthorised modification of system-verified data.
- 4.3.5. The System shall maintain a complete eligibility status history for each entity (company or individual), including all check results, timestamps, status changes, and remediation actions.
- 4.3.6. The System shall provide configurable rating, classification, or segmentation features (e.g., strategic partner rating, engagement depth classification) editable by authorised users.
- 4.3.7. The System shall provide dashboard views or summary panels within Company Profiles displaying key metrics such as application history, funding amounts, approval amounts, claimed amounts, participant counts, and other configurable indicators.
- 4.3.8. Application Submission
  - (a) The System shall provide an externally accessible Front Portal enabling companies or applicants to independently submit grant applications.
  - (b) The Front Portal shall allow applicants to select from available schemes based on eligibility, application dates, and other configurable criteria.
  - (c) The System shall enable applicants to enter application details, upload supporting documents (e.g. document upload box with drag-and-drop feature), and perform eligibility self-checks via the Front Portal.
  - (d) Once an application is submitted via the Front Portal, the System shall route it to the appropriate internal officer or team based on configurable routing rules (e.g., by scheme, sector, geography, or other attributes).

- (e) The System shall support classification of applications into configurable project types (e.g., strategic vs. standard projects) with associated routing, approval, and funding treatment rules.
- (f) The System shall provide configurable data governance rules controlling which fields can be edited by internal officers after submission, ensuring data integrity while supporting case management flexibility.
- (g) The System shall support generation and download of application forms in configurable document formats (e.g., DOCX for editable draft versions, PDF for submitted or locked versions), with format availability dependent on application status and user role.
- (h) The System shall not require all applications to be entered by internal officers; the Front Portal shall be the primary channel for new applications, with backend entry limited to exceptional circumstances or legacy data.

#### 4.3.9. Project Tranches

- (a) The System shall enable authorised users to define the number of project tranches for an application, along with the allocation of funding amounts, timelines, and conditions per tranche.
- (b) The System shall support configurable tranche activation rules, such as sequential activation (one tranche activates after the previous is fully disbursed or closed) or conditional activation based on milestones.
- (c) The System shall allow authorised users to cancel, delete, or modify tranches subject to configurable business rules, with automatic adjustment of fund balances.
- (d) The System shall support the application of Project Variations to individual project tranches rather than entire applications, where applicable.

#### 4.3.10. Project Variation Submission

- (a) The System shall allow applicants to submit Project Variation (PV) requests via Front Portal for all eligible applications, subject to configurable eligibility rules.
- (b) The System shall support classification of Project Variations into configurable categories (e.g., cost-related vs. non-cost-related, timeline extensions, scope changes) with each category having distinct approval routing and business rules.
- (c) The System shall apply configurable routing rules for cost-related variations, with routing determined by factors including:
  - Direction of cost change (increase vs. decrease)

- Magnitude of change (absolute or percentage)
  - Original approval authority
  - Aggregated budget rules
  - Project classification
- (d) The System shall enforce configurable business rules for determining whether a variation requires escalation to a higher approval authority or can be approved by the original approving authority.
- (e) The System shall support generation and download of PV forms in configurable document formats, with format availability dependent on PV status and user role.
- (f) The System shall NOT require all PV requests to be entered by internal officers; the Front Portal shall be the primary channel for PV submissions, with backend entry limited to exceptional circumstances.

#### 4.3.11. Claim Submission

- (a) The System shall enable applicants to submit claims via the Front Portal once the related project or tranche has reached an eligible status (as defined by configurable business rules).
- (b) The System shall support claim submissions under multiple configurable claim categories or funding components, with each category having distinct validation rules, approval workflows, and supporting document requirements.
- (c) Typical claim categories may include:
- Course Fees
  - Salary Support
  - In-House Training
  - Absentee Payroll
  - Training Allowance
  - Other funding components defined by the e2i
- (d) The System shall support configurable field visibility and editability rules for the Front Portal, ensuring applicants see only relevant fields and cannot access or modify internal processing fields.
- (e) The System shall enforce configurable business rules preventing claim submissions when conflicting transactions are in progress for the same project or tranche.
- (f) The System shall support multiple concurrent claim submissions for different tranches, categories, or funding components based on configurable concurrency rules.

- (g) The System shall support generation and download of claim forms in configurable document formats, with format availability dependent on claim status and user role.
- (h) The System shall not require all claims to be entered by internal officers; Front Portal shall be the primary channel for claim submissions, with backend entry limited to exceptional circumstances or legacy transactions.

#### 4.4. Grant Administration

##### 4.4.1. General Workflow Requirements

- (a) The System shall implement a fully configurable, multi-level approval workflow supporting diverse approval scenarios for applications, project variations, claims, and other transactions.
- (b) The System shall support configurable round robin assignment of cases to designated officers or teams. Assignment rules shall be configurable based on parameters such as current case load, officer availability, role, and workload thresholds to ensure balanced and efficient distribution of cases.
- (c) The System shall support but not limited to the following workflow actions at each approval stage, with action availability configurable per role and transaction type:
  - Support (route to next approver without final approval authority)
  - Approve (if approver has sufficient authority)
  - Reject (with mandatory justification)
  - Request More Information (with ability to specify the target role or user)
  - Declare Conflict of Interest and trigger reassignment
  - Withdraw or Cancel (subject to business rules)
  - Terminate (for application termination post outcome from investigation)
- (d) The System shall support dynamic routing of transactions based on configurable criteria including but not limited to:
  - Transaction amount (absolute or aggregated)
  - Scheme type
  - Project classification
  - Applicant attributes
  - Historical funding amounts within defined periods
- (e) The System shall support configurable approval matrices defining:

- Approval authorities by role or named individual
  - Approval limits per authority matrixes for varying modules (e.g. Applications, Project Variation and Claims)
  - Escalation rules when limits are exceeded
  - Budget aggregation rules for calculating total exposure across multiple applications or time periods
- (f) The System shall support delegation of approval authority from one user to another, with defined delegation periods, scope limitations, and audit trails.
- (g) The System shall support oversight and reporting mechanisms for delegated approvals, enabling senior authorities to review decisions made under delegation.

#### 4.4.2. Application Approval Workflow

- (a) The Application Approval workflow shall be configurable to proceed through multiple sequential or parallel stages, with roles, sequence, and conditions defined by the e2i.
- (b) Typical workflow stages may include but are not limited to:
- Application Submission (by Applicant or Officer)
  - Application Review (by Partnership Group Officer)
  - Team Lead Review
  - First Reviewer (Reviewer role)
  - Second Reviewer (Checker role)
  - Approvers at various authority levels (Team Lead, Deputy Chief Executive, Chief Executive, Board-level, or other defined authorities)
- (c) At each workflow stage, the System shall enable reviewers and approvers to:
- Review application details, supporting documents, and prior evaluations
  - Edit specific fields subject to role-based permissions
  - Upload additional supporting documents
  - Provide comments, recommendations, and justifications
  - Request more information from prior roles
  - Support, Approve, or Reject based on their authority level and business rules
- (d) The System shall track and display application status at each workflow stage using configurable status codes and labels that reflect the current processing stage and responsible role.



- (e) The System shall provide workflow visualisation tools enabling users to view the complete approval path, including completed stages, current stage, pending stages, and estimated completion timeline.

#### 4.4.3. Project Variation Processing and Approval Workflow

- (a) Typical PV workflow stages may include submission, validation, PG OIC review, PG Team Lead/DyCEO support, GPT review/checking, and approval by the relevant authority based on funding impact, exposure, scheme rules, and authority limits.
- (b) At each stage, reviewers and approvers shall be able to review relevant application, project, PV, funding, claim, compliance, document, and validation details.
- (c) The System shall determine whether a PV can proceed, be routed, or be blocked based on configurable conditions such as project/tranche status, LOA/Addendum status, pending claims or PVs, disbursement, closure, compliance/watchlist status, and scheme restrictions.
- (d) For cost-related PVs, the System shall calculate financial impact, including approved funding, commitments, tranche allocations, component caps, balances, returned amounts, and fund availability.
- (e) The System shall route PVs based on configurable conditions such as PV type, funding impact, amount or percentage change, cumulative variation, exposure, approving authority, scheme, project classification, funding component, tranche, sector, or other attributes.
- (f) Upon final PV approval, the System shall update relevant project, tranche, funding, workflow, document, and status records, and trigger Addendum generation, fund adjustments, financial updates, notifications, and audit trails where applicable.
- (g) The System shall provide PV workflow visualisation showing the approval path, completed/current/pending stages, responsible users/roles, timestamps, comments, decisions, and estimated completion timeline.

#### 4.4.4. Claims Processing and Approval Workflow

- (a) The System shall implement a configurable Claims approval workflow with routing determined by claim amounts, claim types, scheme parameters, and payment approving authority matrices.
- (b) The System shall enforce configurable business rules preventing claim submissions when conflicting transactions are in progress (e.g., pending project variations for the same tranche).



- (c) The System shall support multiple concurrent claim submissions for different tranches, claim categories, or funding components, subject to configurable concurrency rules.
- (d) Upon claim approval by the final payment approving authority, the System shall trigger configurable notifications to finance staff and initiate the disbursement process.
- (e) The System shall validate claim amounts against approved funding amounts, scheme caps, tranche balances, past claim transactions for duplicated claims in system and other configurable validation rules before allowing submission.
- (f) The System shall support claim withdrawal by applicants or authorised officers, with configurable withdrawal approval workflows based on claim processing stage.

#### 4.5. Vendor and Purchase Order (PO) Creation and Management

- 4.5.1. The System shall integrate with enterprise financial systems to create Vendors and Purchase Orders and allow for adjustments made. Refer to section **Error! Reference source not found. Error! Reference source not found.** for more information.
- 4.5.2. The System shall allow configuration of API trigger point for vendors and PO creation to enterprise financial systems based on business scenarios.

#### 4.6. Invoice and Disbursement

- 4.6.1. Upon claim approval, the System shall create invoice records or payment instructions in the enterprise financial system via API integration. Refer to **Error! Reference source not found. Error! Reference source not found.** for details.
- 4.6.2. Upon successful disbursement, the System shall send configurable notifications to relevant stakeholders (applicants, officers, approvers) via email, in-app notifications, or other configured channels.
- 4.6.3. The System shall support distinct processing and notification workflows for different claim types or funding components.
- 4.6.4. The System shall support manual triggering of financial adjustment notices (e.g., credit notes, debit notes) by authorised users based on configurable business scenarios.

#### 4.7. Forms and Digital Letters Generation and Signature

#### 4.7.1. Forms Generation

- (a) The System shall support configurable forms across all applicable modules, including but not limited to application, project variation, claims, and company profile maintenance. Authorised users shall be able to customise form fields, add or configure document upload boxes, apply validation rules, and define mandatory or optional fields without code changes.
- (b) The forms shall be linked to scheme parameter settings, so that field visibility, mandatory fields, document requirements, validation rules, dynamic data population, and signature requirements can be configured based on scheme type, funding component, transaction type, user role, and transaction status.
- (c) The System shall support dynamic fields that can retrieve, display, or pre-populate data from other modules within the System, including company profiles, application records, project variations, claims, scheme parameters, approval workflows, and integration results. The System shall also support configurable declaration, acknowledgement, electronic signature, or digital signature features where required, with version control and audit trails for all form configurations and submissions.

#### 4.7.2. LOA Issuance

- (a) Upon application approval, the System shall automatically generate a Letter of Award (LOA) or equivalent approval document based on pre-configured, customisable templates.
- (b) The System shall support different LOA issuance policies based on project classification (e.g., immediate issuance for strategic projects, conditional or phased issuance for standard projects).
- (c) The System shall support issuance of alternative approval documents such as In-Principal Approval (IPA) letters, conditional approvals, or phased approvals based on configurable business rules.
- (d) The System shall track LOA status throughout the application lifecycle using configurable status values, supporting scenarios including pending endorsement, endorsed, lapsed, voided, extension, and other states defined by the e2i.
- (e) The System shall support LOA Extension requests initiated by applicants or officers, with extension approval workflows and configurable extension limits.

- (f) The System shall define and enforce configurable LOA acceptance periods, extension periods, and lapse rules.
- (g) The System shall automatically mark LOA as "Lapsed" when configured expiry dates or extended expiry dates are reached.
- (h) The System shall send configurable reminder notifications at defined intervals before LOA expiry.
- (i) The System shall enforce configurable business rules when LOA lapses, including automatic project withdrawal, status change, or manual intervention requirements, with different rules applied based on project classification.
- (j) The System shall support LOA editing and regeneration by authorised users before or after issuance, with version control and audit trails.

#### 4.7.3. Addendum Issuance

- (a) Upon PV approval, the System shall automatically generate an Addendum to the original LOA or issue a new approval document based on configurable business rules.
- (b) The System shall support Addendum editing, version control, and regeneration by authorised users.
- (c) The System shall support Addendum Extension requests with configurable acceptance periods, approval workflows, and lapse rules.
- (d) The System shall automatically adjust fund balances (pipeline amounts, approved amounts, available balances) based on approved cost variations.

#### 4.7.4. Document Template Management

- (a) The System shall provide a comprehensive Document Template Management module enabling authorised users to create, edit, version-control, approve, and retire document templates for:
  - Application forms and letters
  - Letters of Award (LOA)
  - In-Principal Approval (IPA) letters
  - Addendums and amendments
  - Claim forms and payment notices
  - Closure notifications
  - Email notifications
  - Reports and certificates
  - Other business documents as defined by the e2i

- (b) The System shall support dynamic field population within templates, automatically inserting data from application records, company profiles, scheme parameters, user profiles, and other system entities.
- (c) The System shall support configurable data fields within the form, with the configurable validation checks for data integrity.
- (d) The System shall support conditional logic, loops, and complex formatting within templates to display or hide sections based on configurable criteria (e.g., project type, scheme, funding components, applicant attributes).
- (e) The System shall maintain version history for all templates, with the ability to revert to previous versions, compare versions, and apply specific template versions to historical transactions.
- (f) The System shall support multi-format document generation (PDF, DOCX, HTML, and other formats as required) based on user role, document status, and business requirements.
- (g) The system should support Digital Signature through Singpass or Corppass.

#### 4.8. Project and Grant Closure Management

##### 4.8.1. Closure Types and Workflows

- (a) The System shall support multiple configurable closure types for applications and project tranches, with each closure type having distinct triggers, eligibility rules, approval workflows, and financial impacts. Typical closure types may include but are not limited to:
  - **Application Withdrawal:** Applicant-initiated or officer-initiated withdrawal with configurable validation rules ensuring no conflicting transactions are in progress
  - **Termination:** Officer-initiated termination with approval workflow, subject to configurable eligibility rules
  - **Pre-mature Closure:** Early closure before scheduled completion date, with approval workflow and configurable fund return rules
  - **Standard Closure:** Closure at or after scheduled completion date, with approval workflow and configurable fund return rules
  - **Main Application Closure:** Closure of entire application affecting all tranches, with comprehensive eligibility checks and fund return rules

- (b) The System shall automatically calculate and process fund returns based on configurable rules, returning unclaimed or unused funds to the appropriate fund entity (scheme fund pot, grant fund pot, tranche-level unused balance, or other defined destination).
- (c) The System shall enforce configurable document requirements for closure actions (e.g., closure reports, completion certificates, supporting evidence).
- (d) Upon closure, the System shall trigger configurable actions in integrated systems, such as closing related purchase orders, updating candidate status, or archiving records.
- (e) The System shall support configurable approval workflows for withdrawal requests initiated by applicants, with different workflows based on application processing stage (e.g., automatic withdrawal for unapproved applications, approval workflow for approved applications).
- (f) The System shall allow applicants to cancel their withdrawal request at any point before final approval, subject to configurable business rules.

#### 4.8.2. Grant Recovery and Clawback

- (a) The System shall support grant recovery (clawback) functionality for scenarios where participants drop out, fail to meet commitments, breach programme terms, or trigger other recovery conditions defined by policy.
- (b) The System shall calculate the grant amount to be recovered based on configurable recovery rules, with rules supporting:
  - Pro-rated recovery based on completion percentage, drop-out point, or other milestones
  - Full recovery of specific funding components
  - Partial recovery with defined calculation logic
  - Conditional recovery based on participant circumstances or mitigating factors
- (c) The System shall maintain a recovery tracking module recording all recovery actions, amounts, contact attempts, payment statuses, instalments, write-off requests, and approvals.
- (d) Write-off requests for unrecoverable grant amounts shall follow configurable approval workflows based on write-off amounts and approving authority matrices.
- (e) The System shall support configurable policies for interest or penalties on grant receivables, with the ability to waive or apply such charges based on defined criteria.

#### 4.9. Candidate Onboarding and Endorsement

##### 4.9.1. Candidate Onboarding

- (a) The System shall integrate with candidate management or master data systems to retrieve, synchronise, and update candidate or participant information.
- (b) The System shall provide interfaces or forms enabling authorised officers to enter or update candidate onboarding details including personal information, programme details, placement information, salary information, and funding calculations.
- (c) Upon candidate data entry or update, the System shall route the information through configurable approval or endorsement workflows.
- (d) Before candidate endorsement, the System shall perform configurable validation checks including but not limited to:
  - Blacklist verification against multiple sources
  - Supporting document completeness checks
  - Programme quota or allocation checks
  - Funding cap or budget checks
  - Salary or wage verification against declared or approved amounts
  - Other eligibility or compliance checks defined by policy
- (e) Upon successful candidate endorsement, the System shall automatically adjust fund balances based on configurable rules (e.g., moving funds from uncommitted to committed status, generating financial commitments).
- (f) The System shall support batch endorsement of multiple candidates, with configurable document generation (e.g., one LOA per batch or one LOA per candidate).
- (g) The System shall automatically update candidate status via API from integrated candidate management or master data systems upon endorsement approval or status changes.

##### 4.9.2. Post-Endorsement Candidate Status Management

- (a) The System shall support configurable candidate lifecycle status transitions with each status change triggering defined business rules including validation, fund adjustments, notifications, and integration updates.
- (b) Typical candidate statuses may include but are not limited to:
  - Pending PO Action

- Pending AO Action
  - Pending Grantor Action (Review)
  - Pending Company Action
  - Pending System Action
  - Pending Acceptance of Offer
  - Offered Acceptance
  - Training Status Updating
  - Pending WSG Action (Terminate)
  - Withdrawn
  - Rejected
  - Offered Rejected
  - Terminated
  - Training Completed
  - Offered and Withdrawn
  - Training Dropped-Out
  - Other statuses defined by the e2i
- (c) Each status transition shall support configurable rules including:
- Document requirements
  - Fund movement or reversal logic
  - Quota or allocation adjustments
  - Claim eligibility rules
  - Integration synchronisation requirements
- (d) The System shall synchronise all candidate status changes with integrated systems in real-time or near-real-time based on configured integration patterns.
- (e) The System shall support configurable approval requirements for candidate status changes, with the ability to require approvals for certain transitions and allow automatic transitions for others.

#### 4.10. Statement of Grant Claim (SOGC)

##### 4.10.1. SOGC Module Overview.

The System shall provide a SOGC module to manage the audit cycle for grant claims. It shall flag claims by company UEN based on configurable business rules, maintain audit tracking records, and support GRC users in managing audit requests, document submissions, reimbursement claims, reviews, outcomes, and closure.



- 4.10.2. The System shall provide a SOGC worklist for GRC users to view, filter, assign, and track flagged companies and claims by UEN, scheme, claim type, audit cycle, risk indicator, status, officer, due date, and ageing.
- 4.10.3. The System shall allow GRC users to create, update, assign, escalate, hold, cancel, or close SOGC cases, subject to role-based access, approval rules, and mandatory justifications.
- 4.10.4. Upon case approval or activation, the System shall notify the company through the Front Portal, email, in-app notification, or other approved channels on the audit request, required documents, submission deadline, reimbursement eligibility, and reimbursement cap.
- 4.10.5. The System shall allow companies to submit audit documents and reimbursement claims via the Front Portal within the stipulated period, with validation against document requirements, file formats, declarations, claim categories, and reimbursement cap.
- 4.10.6. The System shall route submissions to the assigned GRC officer for review, clarification, recommendation, and further approval based on configurable workflow rules.
- 4.10.7. The System shall support configurable SOGC statuses, including Flagged, Pending GRC Review, Pending Approval, Pending Company Submission, Pending Clarification, Under Review, Claim Submitted, Approved, Rejected, Closed, Cancelled, and Overdue.
- 4.10.8. The System shall generate reminders, overdue alerts, escalation notifications, and task summaries based on configurable due dates, service standards, audit timelines, and submission deadlines.
- 4.10.9. The System shall maintain an audit trail of SOGC activities, including flagging, case creation, assignment, approvals, notifications, submissions, review comments, status changes, decisions, closure actions, timestamps, and user actions.

#### 4.11. Workflow Management and Notifications

##### 4.11.1. Workflow Engine

The System shall implement a fully configurable workflow engine enabling authorised users to define, modify, test, activate, and deactivate workflows without code deployment or system downtime.

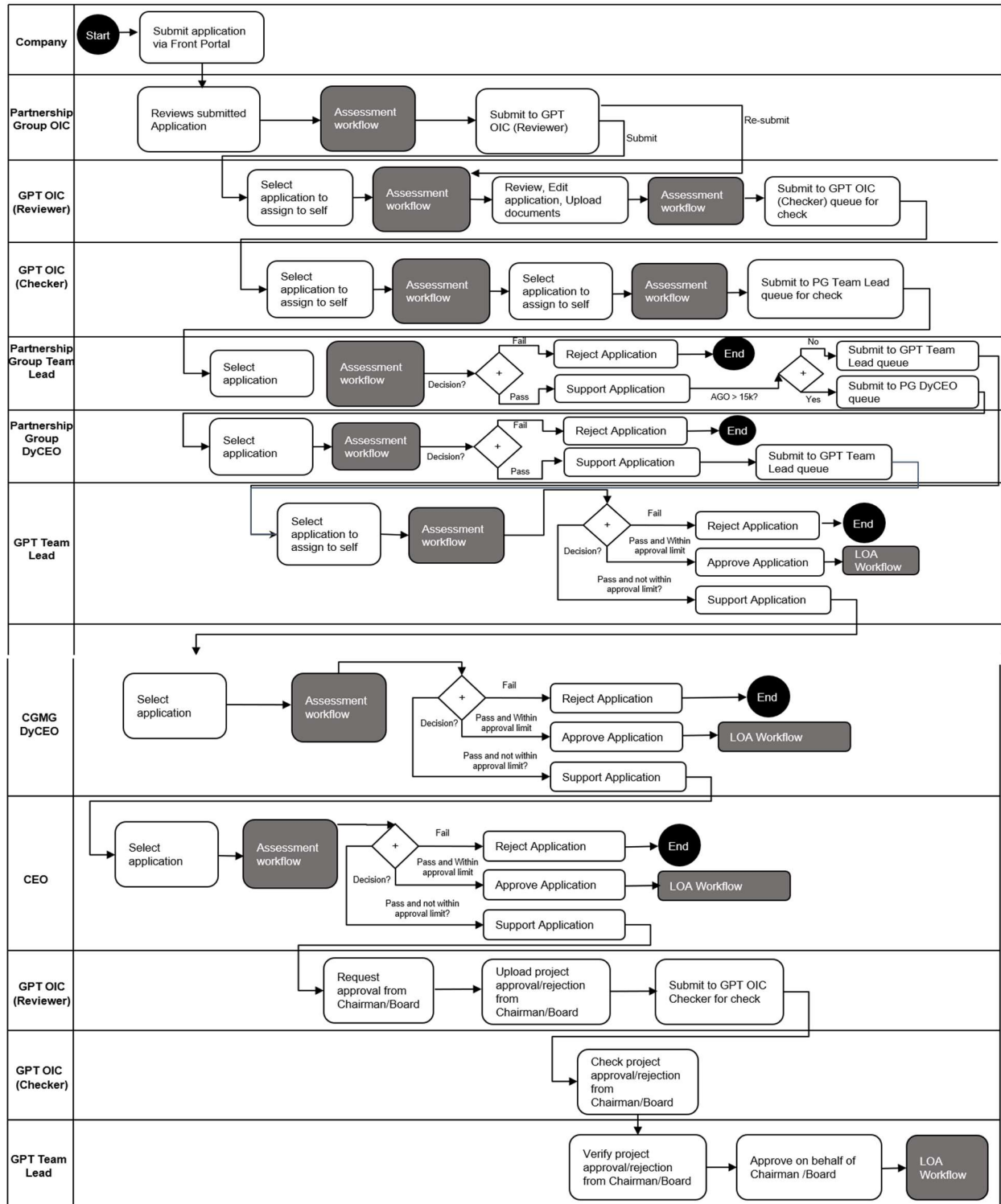
##### 4.11.2. The workflow engine shall support diverse routing patterns including:

- (a) Sequential routing (step-by-step progression through defined stages)



- (b) Parallel routing (multiple approvers at the same level, all approvals required or majority required)
  - (c) Conditional routing (based on transaction attributes, amounts, thresholds, or other configurable criteria)
  - (d) Dynamic routing (routing destination determined at runtime based on rules engine evaluation)
  - (e) Escalation rules (automatic routing if approval not completed within defined timeframes)
  - (f) Reassignment (manual or automatic transfer to another user or role)
- 4.11.3. Workflows shall support configurable actions at each stage, with action availability controlled by role and business rules, including but not limited to: Approve, Reject, Support, Require More Information, Declare Conflict of Interest, Withdraw, Terminate, Defer, Delegate.
- 4.11.4. The System shall provide workflow visualisation tools displaying the current workflow path, completed stages, current stage, pending stages, estimated completion timeline, and historical workflow execution for each transaction.
- 4.11.5. The System shall maintain a comprehensive workflow audit trail recording all workflow transitions, actions taken, users involved, timestamps, comments, justifications, and system-generated events.

#### 4.11.6. Sample workflow as depicted below:



4.11.7. Notification and Alerting

The System shall send automated notifications for configurable business events as specified in the notification configuration, with each event supporting customisable notification templates, recipient determination rules, and delivery channels.

4.11.8. The System shall support scheduled notifications (daily, weekly, monthly, or other defined frequencies) sent at configurable times, summarising pending tasks, approaching deadlines, overdue items, performance metrics, and other actionable or informational content.

4.11.9. Email Notifications

- (a) The System shall send automated email notifications for configurable business events, with each event having customisable notification templates, recipient lists, and delivery rules.
- (b) Typical notification events may include but are not limited to:
  - Application or claim received acknowledgments
  - Approval or rejection notifications
  - Clarification or information requests
  - Document issuance (LOA, IPA, Addendum, etc.)
  - Reminder notifications for approaching deadlines
  - Lapse or expiry notifications
  - Disbursement confirmations
  - Closure notifications
  - Candidate endorsement notifications
  - Daily or periodic task summaries
  - Escalation alerts
  - Fund utilisation threshold alerts
  - Tasks Summary catered to individual users
  - Vendor, PO, and Invoice creation
  - API Driven Error Notification Emails
  - Claw back notifications
- (c) Email notifications shall support configurable recipient routing (To, CC, BCC) based on event type, transaction attributes, organisational hierarchy, and stakeholder involvement.
- (d) The System shall support scheduled notifications (daily, weekly, monthly, or other defined frequencies) sent at configurable times,

summarising pending tasks, approaching deadlines, overdue items, and other actionable information.

- (e) Email templates shall be fully configurable by authorised users, supporting dynamic field insertion, embedded links to relevant forms, conditional logic, formatting, attachments, and multi-language content.
- (f) The System shall maintain a comprehensive email notification log recording all sent notifications, recipients, timestamps, delivery status, bounce notifications, and failure reasons.
- (g) The System shall support email delivery retry mechanisms and failure alerting to ensure critical notifications reach intended recipients.

#### 4.11.10. In-App Notifications and Task Management

- (a) The System shall provide an in-app notification centre displaying real-time alerts, pending tasks, action items, and messages for each logged-in user.
- (b) The System shall provide role-based landing dashboards showing actions, alerts, follow-ups, key performance indicators, and other relevant information tailored to each user role.
- (c) The System shall support configurable task escalation alerts when tasks remain pending beyond defined time thresholds, with escalation routing to supervisors or higher authorities.

### 4.12. Reassignment and Conflict of Interest Management

#### 4.12.1. Project Reassignment

- (a) The System shall support reassignment of transaction ownership or responsibility from one user to another, with configurable reassignment rules based on role, transaction type, and organisational structure.
- (b) The System shall automatically update relevant transaction attributes (e.g., sector, subsector, team assignment) upon reassignment based on the new owner's profile.
- (c) The System shall support two reassignment modes:
  - **Administrative Reassignment:** Administrators or supervisors can reassign across roles and organisational boundaries
  - **Peer Reassignment:** Users can reassign within their role or team subject to configurable restrictions
- (d) The System shall enforce configurable reassignment rules defining which roles can reassign to which other roles, with optional restrictions based on organisational attributes (e.g., sector, geography, programme).

#### 4.12.2. Conflict of Interest (COI) Declaration

- (a) The System shall enable users to declare Conflict of Interest at any point during transaction processing, triggering mandatory reassignment workflows.
- (b) Upon COI declaration, the System shall automatically initiate reassignment workflows based on configurable COI reassignment rules, with rules defining eligible replacement roles, escalation paths, and approval requirements.
- (c) The System shall maintain a comprehensive COI declaration log recording all declarations, timestamps, declaring users, affected transactions, reassignment outcomes, and any subsequent actions.
- (d) The System shall enforce configurable access restrictions preventing the declaring user from accessing the affected transaction once COI is declared and reassignment is completed.
- (e) The System should support COI declaration review and approval workflows for sensitive cases, allowing senior authorities to review and approve COI declarations before enforcing access restrictions.

#### 4.13. Watchlist and Compliance Management

- 4.13.1. The System shall provide a Watchlist or Compliance Management module enabling authorised users to upload, maintain, and manage watchlists, blacklists, or other compliance reference lists.
- 4.13.2. The System shall support configurable watchlist classification, status values, severity indicators, and display rules (e.g., colour-coding, alerts).
- 4.13.3. The System shall run configurable scheduled processes to update watchlist status for in-process transactions based on the latest uploaded watchlist data.
- 4.13.4. The System shall enforce configurable rules for when to stop updating watchlist status (e.g., upon reaching defined end states or closure).
- 4.13.5. The System shall support configurable watchlist expiry rules, automatically removing or updating watchlist status when expiry dates are reached.
- 4.13.6. Upon upload of a new watchlist file, the System shall support immediate or scheduled reprocessing of all relevant transactions to update their watchlist status.
- 4.13.7. The System shall check all new applications, claims, variations, and other transactions against the latest watchlist data and assign appropriate status indicators.

- 4.13.8. The System shall display watchlist status prominently on transaction records with configurable visual indicators (colour-coding, icons, alerts), enabling officers to quickly identify compliance issues.
- 4.13.9. The System shall support watchlist checks using configurable identifiers, including but not limited to Unique Entity Number (UEN), National Registration Identity Card (NRIC), and any other relevant entity or individual identifiers as defined by e2i.

#### 4.14. Integration with External Systems

##### 4.14.1. Authentication Providers

- (a) The System shall integrate with the organisational identity provider for internal staff authentication using standard protocols (SAML 2.0, OpenID Connect, OAuth 2.0, or other agreed protocols).
- (b) The System shall integrate with national or government-approved individual digital identity systems (such as Singpass, Corppass) using published APIs and integration specifications.
- (c) The System shall retrieve company or individual profile data from trusted government or commercial data services (such as MyInfo Business API) upon authentication, synchronising data fields as defined by the e2i.
- (d) All authentication integrations shall be tested in staging or testing environments before production deployment, using test accounts, sandbox environments, or testing facilities provided by the respective authentication providers.

##### 4.14.2. Eligibility Verification Services

- (a) The System shall integrate with statutory or regulatory systems to verify live company status, registration details, and compliance status in real-time or near-real-time such as ACRA API Services.
- (b) The System shall integrate with compliance or blacklist verification systems to verify company and individual blacklist status, eligibility status, and compliance standing such as SWDA Blacklist API or equivalent.
- (c) Eligibility check API calls shall complete within timeframes defined in the SLA, with timeout and configurable retry mechanisms.
- (d) The System shall handle API failures gracefully, logging errors, alerting administrators, and providing fallback mechanisms (e.g., manual override by authorised users with justification, queuing for retry, or alternative verification methods).

- (e) The System shall implement caching strategies for eligibility check results to reduce API call frequency and improve performance, with cache expiry periods configurable based on data volatility and business requirements.
- (f) The System shall support configurable downstream handling rules, system-wide, for applications, project variations, claims processing, and company profile maintenance based on the statuses, outcomes, or indicators returned by interfacing systems.
- (g) The System shall include the capability for authorised users to configure and manage whitelisting, blacklisting, and de-blacklisting rules and actions at the company profile level and, where applicable, at the individual application, project variation, and claim levels.
- (h) The System shall apply such configurations to determine the appropriate downstream actions, including but not limited to allowing processing to proceed, preventing further submission or approval, routing for manual review, triggering notifications, updating relevant statuses, and maintaining a complete audit trail of all rule configurations, status changes, overrides, and user actions.

#### 4.14.3. Financial System Integration

- (a) The System shall integrate with enterprise financial systems (including but not limited to SAP S/4 HANA or equivalent ERP systems) for Purchase Order (PO) creation, PO adjustments, invoice creation, payment processing, and disbursement confirmation.
- (b) All financial system integration transactions shall prevent duplicate POs, invoices, or disbursements in case of retry, timeout, or network failures.
- (c) The System shall maintain a reconciliation capability comparing GMS records with enterprise financial system records (PO amounts, invoice amounts, disbursement amounts), with alerts for discrepancies exceeding defined thresholds.
- (d) The System shall support API error handling with necessary return API error messages and notifications, and extraction of payload by authorised users.

#### 4.14.4. Claims Processing Platform Integration

- (a) The System shall support integration with external claim verification, assessment, and approval platforms, including but not limited to



SWDA's TP Gateway (e-Serv), through secure APIs or other approved integration mechanisms.

- (b) The System shall be capable of receiving and processing claim verification outcomes, approval decisions, disbursement instructions, status updates, and other claim-related transactions from external claim processing platforms.
- (c) Upon receipt of a successful verification or approval outcome from an external claim processing platform, the System shall automatically update the relevant claim records and initiate the subsequent disbursement workflow in accordance with e2i's configured business rules, approval matrix, delegation of authority, and governance requirements.
- (d) The System shall support configurable workflow routings to ensure that claim disbursement approvals continue to follow e2i's internal approval matrix and authority limits, irrespective of the approval or verification process performed by external platforms.
- (e) The System shall provide configurable retry mechanisms, exception handling, error logging, and administrator notifications for failed or delayed transactions with external claim processing platforms.

- 4.14.5. Signing with Corppass and Singpass. The system should use Sign (a digital signing solution built on the Corppass and Singpass ecosystem) to allow users to sign documents such as contracts and other agreements remotely, via their Corppass and Singpass App.

#### 4.15. Standard Reports

- 4.15.1. The System shall provide a library of pre-built standard downloadable reports addressing common operational, management, compliance, and statutory reporting needs. Report categories may include:
  - (a) Master data report
  - (b) Programme and placement reports
  - (c) Participant listings and demographic analysis
  - (d) Project attachments, allocations, and status reports
  - (e) Productivity, outcome, and impact tracking
  - (f) Compliance and audit reports (blacklist reports, eligibility reports, violation reports)



- (g) Company listings and engagement summaries reports
    - (h) Financial reports (commitments, pipeline, disbursements, recoveries, fund balances)
    - (i) Statutory or regulatory reports required by funding bodies or government agencies
  - 4.15.2. All reports shall support configurable filtering by multiple dimensions and attributes relevant to the report, with filter options saved and reusable for future report executions.
  - 4.15.3. Pre-built standard reports shall be configurable to include new or revised fields arising from changes to the relevant form changes.
  - 4.15.4. The System shall support report export in multiple configurable formats (e.g. .XLSX, .CSV, .PDF) to accommodate different use cases (viewing, printing, data analysis, archival).
  - 4.15.5. The System shall provide drill-down capabilities within reports, enabling users to navigate from summary aggregations to detailed record views, and from detailed records to the full transaction in the system.
  - 4.15.6. The System should integrate with external analytics, business intelligence, or master data systems where reporting data is consolidated across multiple systems or where centralised reporting infrastructure exists.
- 4.16. Ad-hoc Reporting and Data Export
- 4.16.1. The System shall provide an ad-hoc report builder or self-service business intelligence tool enabling authorised users to create, execute, save, and share custom reports without IT intervention.
  - 4.16.2. The ad-hoc report builder shall support:
    - (a) Drag-and-drop or wizard-based field selection from available data entities
    - (b) Filtering by multiple criteria with complex boolean logic (AND/OR/NOT combinations)
    - (c) Grouping, sorting, and multi-level aggregation (SUM, COUNT, AVG, MIN, MAX, MEDIAN, DISTINCT COUNT, etc.)
    - (d) Calculated fields using formulas, expressions, and functions
    - (e) Chart and graph visualisation with multiple chart types (bar, line, pie, scatter, heat map, treemap, etc.)
    - (f) Conditional formatting and styling
    - (g) Report parameterisation for dynamic filtering at runtime

- 4.16.3. The System shall support scheduled report generation and automated distribution via email or other configured channels to designated recipients at defined intervals (daily, weekly, monthly, quarterly, or custom schedules).
  - 4.16.4. The System shall provide a data export facility enabling authorised users to export filtered datasets or query results for external analysis, reporting, or integration, subject to role-based access controls and data security policies.
  - 4.16.5. The System shall limit ad-hoc report and data export execution time to prevent system performance degradation; reports or exports exceeding defined time thresholds shall be queued for background processing with notification upon completion.
  - 4.16.6. All data exports shall respect role-based access controls, data masking rules, and data protection policies, ensuring users can only export data they are authorised to view.
  - 4.16.7. The System shall maintain a comprehensive audit log of all report generation, execution, data export, and report sharing activities, including user, timestamp, report type, filters applied, export format, recipients, and execution results.
- 4.17. Dashboards and KPIs
- 4.17.1. The System shall provide role-based landing dashboards displaying key performance indicators (KPIs), actionable widgets, alerts, and other information tailored to each user role.
  - 4.17.2. Dashboard KPIs and widgets shall be configurable by authorised administrators and may include (role-dependent):
    - (a) Application and claim submission volumes (by period)
    - (b) Applications and claims pending approval (by stage, by age, by priority)
    - (c) Approval rates, rejection rates, and average processing times
    - (d) Aging projects
    - (e) Application, onboarding, claims projection
    - (f) Funding committed, funding disbursed, and funding pipeline
    - (g) Fund balances, fund utilisation, and forecasted commitments
    - (h) Project completion rates and closure rates
    - (i) Recovery and clawback amounts
    - (j) Compliance indicators (blacklist hits, eligibility failures, overdue tasks)
    - (k) User productivity metrics (transactions processed, approvals completed)
    - (l) Cashflow projection

- 4.17.3. Dashboard widgets shall update in real-time or near-real-time with refresh intervals configurable per widget, dashboard, or user preference. Authorised users shall be able to personalise, drag and drop, save, manage, set as default, and reset dashboard views according to individual preferences, using dashboard components, KPIs, filters, widgets, layouts, and refresh intervals made available to their role, subject to role-based access controls, data governance rules, and system performance controls.
  - 4.17.4. The System shall provide configurable data visualisation tools for dashboard widgets, enabling authorised users to present available KPIs and data using suitable visual formats such as bar charts, line charts, pie charts, tables, counters, trend indicators, and other approved visualisation types, subject to role-based access controls and data governance rules.
  - 4.17.5. Dashboard widgets shall support drill-down, enabling users to navigate from summary KPIs to detailed underlying records, filtered views, or related reports.
  - 4.17.6. The System shall support dashboard downloads in Power BI-compatible or equivalent formats, including (CSV, PPT, XLSX, PDF, PBIX) and other configurable formats.
- 4.18. Business Rules Engine
- 4.18.1. The System shall provide a comprehensive, configurable Business Rules Engine enabling authorised users to define, edit, test, control, activate, and deactivate business rules without code deployment or system downtime.
  - 4.18.2. The Business Rules Engine shall support rule definition for:
    - (a) Eligibility criteria based on applicant attributes, project attributes, scheme parameters, and external data
    - (b) Funding calculation formulas for all funding components (course fees, salary support, training allowance, and other defined components)
    - (c) Approval routing logic based on transaction amounts, aggregation rules, project classification, scheme type, and organisational hierarchy
    - (d) Validation rules for applications, claims, project variations, candidate data, and other transactions
    - (e) Notification triggers, recipient determination, and content personalisation
    - (f) Workflow actions, transitions, and conditions
    - (g) Fund allocation, commitment, and return logic
    - (h) Status determination and progression rules
  - 4.18.3. The Rules Engine shall support logic including:
    - (a) Conditional statements (IF-THEN-ELSE, nested conditions)

- (b) Mathematical operations (addition, subtraction, multiplication, division, percentages, rounding)
  - (c) Date and time calculations (age calculation, duration calculation, date comparisons)
  - (d) String manipulations (concatenation, substring, pattern matching)
  - (e) Lookups to reference data tables, external systems, or master data
  - (f) Recursive or iterative logic where applicable
- 4.18.4. The System shall support rule versioning with effective-from and effective-to dates, enabling multiple rule versions to coexist and apply to different time periods, ensuring historical transactions use historical rules and new transactions use current rules.
- 4.18.5. The System shall provide a rule testing or simulation environment where authorised users can test rule changes against sample data, historical data, or hypothetical scenarios before activating rules in production.
- 4.18.6. The System shall maintain a comprehensive audit trail of all rule changes, including user, timestamp, rule version, before and after values, and justification for change.
- 4.18.7. The System shall support import and export of rule sets in structured formats (CSV, JSON, XML) to facilitate backup, version control, migration across environments, and disaster recovery.
- 4.19. Data Migration from Legacy Systems
- 4.19.1. The Tenderer shall migrate all historical and active data from existing systems into the new GMS, ensuring operational continuity, historical traceability, audit compliance, and data integrity.
- 4.19.2. Data migration scope shall include all relevant entities defined by the e2i, which may include but are not limited to:
- (a) All grant types, schemes, and associated parameters (including inactive or closed grants required for historical reporting and audit)
  - (b) Historical and active applications, approvals, rejections, withdrawals, terminations
  - (c) Project tranches, variations, addendums, and related documents
  - (d) Claims, disbursements, recoveries, and financial transactions
  - (e) Company profiles, eligibility check history, and CRM records
  - (f) User accounts, role assignments, and access history (where applicable and authorised)
  - (g) Fund management transactions and balances (fund tranches, grants, schemes, allocations, transfers)

- (h) Audit trail records to the extent feasible and appropriate
  - (i) Supporting documents, attachments, and generated documents
- 4.19.3. The Tenderer shall develop a detailed Data Migration Plan including:
- (a) Data mapping specifications (source to target field mappings, transformation rules, default values)
  - (b) Data cleansing, validation, and enrichment rules
  - (c) Migration sequence and dependencies (e.g., master data before transactional data)
  - (d) Validation and reconciliation procedures to ensure migration accuracy
  - (e) Rollback procedures in case of migration failure
  - (f) Migration schedule, cutover plan, and resource requirements
- 4.19.4. The Tenderer shall perform data and records reconciliation between the migrated data in the new GMS and all relevant external integrated systems, including but not limited to financial systems, candidate or participant management systems, authentication and profile data sources, eligibility or compliance verification services, and other systems identified by e2i. The reconciliation shall verify record counts, key identifiers, statuses, financial amounts, transaction references, document references, and other critical fields to ensure consistency, completeness, accuracy, and traceability across systems before production cutover and go-live.
- 4.19.5. The Tenderer shall conduct at least two (2) trial data migrations in a staging or testing environment before the final production migration, with each trial followed by validation, reconciliation, and lessons learned.
- 4.19.6. The Tenderer shall perform comprehensive data quality checks post-migration, including:
- (a) Record count reconciliation (source vs. target)
  - (b) Sample record comparison (manual verification of representative records across all entity types)
  - (c) Business rule validation (e.g., totals match, balances reconcile, status consistency, referential integrity)
  - (d) Referential integrity checks across all related entities
  - (e) Data completeness checks for mandatory fields
- 4.19.7. The Tenderer shall achieve data migration accuracy targets defined by the e2i for critical fields (e.g., entity identifiers, funding amounts, approval dates, disbursement amounts, personal identifiers).
- 4.19.8. The Tenderer shall provide a comprehensive Data Migration Report documenting:

- (a) Number of records migrated by entity type
- (b) Data quality issues identified, resolved, and outstanding
- (c) Validation results and reconciliation summaries
- (d) Outstanding issues and remediation plan (if any)
- (e) Sign-off by e2i

4.19.9. The Tenderer shall ensure source system data is retained in read-only mode or archived for a period defined by the e2i post-migration to support queries, validation, and troubleshooting.

#### 4.20. Data Retention and Archival

- 4.20.1. The System shall retain operational data (active applications, ongoing projects, recent claims, current fund structures) in online storage for periods defined by the e2i.
- 4.20.2. The System shall archive historical data (completed projects, closed applications, old audit logs, obsolete fund structures) to a separate archival storage tier after defined retention periods, while maintaining accessibility for reporting, audit, and compliance purposes.
- 4.20.3. The System shall retain audit trail data for periods defined by the e2i in compliance with audit, regulatory, and legal requirements.
- 4.20.4. The System shall retain financial transaction records (disbursements, recoveries, POs, invoices) for periods defined by the e2i in compliance with accounting standards, tax regulations, and audit requirements.
- 4.20.5. The System shall support data export from archival storage in structured formats (CSV, JSON, XML, database dump, or other agreed formats) for audit, legal discovery, historical analysis, or migration purposes.
- 4.20.6. All documents attached to the operational data, historical data, financial transactions should be exportable from the System in their original format (Word, Excel, pdf or other document formats used in the System)
- 4.20.7. The System shall implement secure data destruction procedures for data beyond retention periods, ensuring complete and irreversible deletion in compliance with data protection regulations and organisational policies.

#### 4.21. Artificial Intelligence Integration

- 4.21.1. The System shall support the integration of Artificial Intelligence (AI) capabilities to improve operational efficiency, decision support, user assistance, data quality, compliance monitoring, reporting, and service responsiveness across the grant management lifecycle. Business scenarios

may include, but are not limited to, AI-enabled user assistance through a chatbot or virtual assistant to guide applicants and officers on application, claim, project variation, and document submission steps; decision-support capabilities (e.g. Optical Character Recognition) to assist authorised users in reviewing application and claims submission completeness, eligibility indicators, funding calculations, routing recommendations, and next-best actions; and compliance monitoring support using Retrieval-Augmented Generation (RAG) to review transaction records, policy documents, audit trails, watchlist results, and supporting documents against applicable grant rules, compliance requirements, and historical precedents.

- 4.21.2. The System shall allow e2i to enable, disable, configure, and monitor AI-enabled functions by module, role, user group, transaction type, scheme, or business process. For example, e2i may enable a chatbot for applicant enquiries, disable AI recommendations for selected schemes, configure RAG sources for compliance review, and monitor AI usage, outputs, exceptions, and user feedback.
- 4.21.3. The Contractor shall ensure that AI integration does not degrade the performance, availability, security, maintainability, or auditability of the System and shall meet the applicable non-functional, security, service management, and SLA requirements defined in this document.

## **5. NON-FUNCTIONAL REQUIREMENTS**

### **5.1. Maintenance Service and Operation Support**

- 5.1.1. The Contractor shall provide Maintenance Service for the System covering day-to-day production/operation support and corrective and preventive maintenance of the System if Maintenance Service is awarded in the Letter of Acceptance. Notwithstanding the foregoing, the Contractor shall provide System such services upon the implementation of the System in Production Environment, at no additional cost to e2i, till end of PGP.
- 5.1.2. The Contractor may designate a separate Project Manager for the Maintenance Service, if agreed by e2i. The Project Manager shall be the single point of contact for Maintenance Services and ensure that all performance indicators in relation thereto in the Contract are met. The Project Manager shall also be in charge of overall management, problem analysis, and resolution of System problems in the Production Environment.
- 5.1.3. e2i may withdraw any part of the System from the coverage under the Maintenance Service by giving a notice of at least thirty (30) calendar days in



writing. The payments to be made for Maintenance Services shall be accordingly reduced based on the item withdrawn.

- 5.1.4. The Contractor shall provide Maintenance Service that include the following:
- (a) provide corrective maintenance, troubleshoot and isolate defects, including diagnosis and correction of all latent errors in the System;
  - (b) investigate and correct defects in the System as reported by e2i, within the Service Levels. The resolution effort for such defects includes, but is not limited to, resolving the errors through developing, testing and implementing changes to the System;
  - (c) assess impact of new releases of software (for example, operating system and security patches) to the System;
  - (d) recover lost data in the System, restore and repair damaged data and correct erroneous data to the extent possible;
  - (e) provide advice, guidance and refresher training to e2i in the use of the System;
  - (f) provide support services, including technical advice and assistance, to ensure continuity, availability and accessibility of the System in Production Environment;
  - (g) implement and enhance operational procedures as and when needed for the System; produce and update the Documentation (including technical and user documentation) for the System in the format and media to be specified by e2i;
  - (h) monitor the System to ensure data integrity and efficient system performance and provide expert advice on performance monitoring and tuning;
  - (i) plan daily operations to ensure optimisation of resources and batch windows utilisation in the System;
  - (j) follow through with the third party vendors for problems that require third party vendors or external organisations for troubleshooting and rectification. These third-party vendors shall include but are not limited to e2i's facilities management ("FM") vendor or any other vendor that provides a service or a product that is related to or Integrated with the System;
  - (k) manage and support changes to the System to minimise impact on system availability;
  - (l) work with e2i's FM vendor or team to provide back-up and recovery services and procedures for the applications and data;
  - (m) provide System briefings to end-users as specified by e2i, or when necessary as determined by e2i;



- (n) prepare technical feasibility proposal including impact analysis, when requested by e2i, for new system functions or enhancements to existing functions in the System;
- (o) provide support for any System security review and audit activities and implement follow-up actions recommended by auditors and consultants engaged by e2i, to maintain and enhance the security of the System; and
- (p) propose improvements to the current work processes and procedures relating to the System, which will result in faster turn-around time and increased efficiency in delivering the Maintenance Services

## 5.2. Problem Management

5.2.1. The Contractor shall follow the problem management procedure endorsed by e2i.

5.2.2. The Service Levels for Response Time (defined below), status reporting and Problem Resolution Time (defined below) are as follows:

| Severity Level | Response Time | Status Reporting          | Problem Resolution Time |
|----------------|---------------|---------------------------|-------------------------|
| 1              | Within 30mins | Every 2 hours             | Within 4 hours          |
| 2              | Within 30mins | Daily                     | Within 3 working days   |
| 3              | Within 30mins | End of Problem Resolution | Within 7 working days   |

5.2.3. “Severity Levels” are priority levels assigned to the problem based on urgency, number of users affected, type and extent of service disrupted and availability of a workaround or fall-back. When a problem is communicated to the Contractor, the Contractor shall assign the Severity Level of the problem based on e2i’s severity definition. e2i reserves the right to re-classify the Severity Levels if the needs arise.

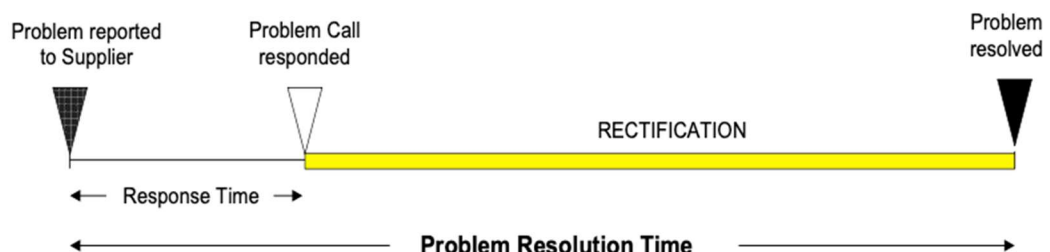
5.2.4. The definition of each Severity Level is as follows:

| Severity Level | Definition |
|----------------|------------|
|----------------|------------|

|                  |                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity Level 1 | These problems affect the System such that e2i is unable to perform its business functions, or cause public alarm or create chaos, or result in negative image or adverse impact on e2i, or result in IT security incidents such as and/or data breach incidents such as hacking or virus attack. |
| Severity Level 2 | These are problems, which affect a particular process, module or sub-system of the System, for which there are existing alternatives to by-pass the problem.                                                                                                                                      |
| Severity Level 3 | These problems have minimal or no impact on e2i's ability to perform its functions.                                                                                                                                                                                                               |

- 5.2.5. The “Response Time” shall begin from the time or date the problem is communicated to the Contractor’s single point of contact, regardless of whether the single point of contact acknowledges receipt of the message. The message may be communicated by any of the e2i’s helpdesks, the e2i’s Representative responsible for the System, or any e2i user through telephone, fax or electronic mail. The “Response Time” ends when a response is provided by the Contractor for the problem via telephone or electronic mail to the person who reports the problem (refer to illustration below).
- 5.2.6. The “Problem Resolution Time” shall begin upon communication of the problem to the Contractor’s single point of contact, regardless of whether the single point of contact acknowledges receipt of the message. The “Problem Resolution Time” ends when the problem is resolved, and the defect is restored to a satisfactorily working condition (refer to illustration below).

#### Illustration of Response Time and Problem Resolution Time



- 5.2.7. The Contractor shall perform a thorough analysis of the problem, which includes identification of the cause of problem, the systems affected, data or any loss suffered and the recommended solution.
- 5.2.8. For Severity Level '1' problems, the Contractor shall provide in writing a preliminary report to explain the incident the following working day. Subsequently the Contractor shall provide a post incident review report to explain in detail the cause of the incident, the corrective actions taken and the solutions to prevent the incident from recurring, within five (5) working days after the incident has been rectified.
- 5.2.9. The Contractor shall provide a mechanism and substantiate to the e2i that Service Levels are met. There must be proper acknowledgement and monitoring of all reported defects and problems by the Contractor. The Contractor shall be responsible to ensure that the e2i's Representative is kept updated on the latest status of the reported defects or problems without being prompted. The frequency of status reporting required is shown in the tables in Paragraph 5.2.2.
- 5.2.10. The Contractor shall work with all parties designated by the e2i and take whatever actions to resolve all problems.
- 5.2.11. In the event of any dispute on the cause of the problem, the Contractor shall demonstrate and prove services rendered within the scope of this Contract are not the cause of the problem. The Contractor shall continue to work with the relevant parties to resolve the problem.
- 5.2.12. The Contractor shall schedule problem reviews to track unresolved problems and provide rectification effort to prevent problem from recurring. e2i shall specify frequency of such reviews.
- 5.2.13. There shall be monthly problem reviews to track unresolved problems and provide rectification efforts to prevent the problem from recurring.
- 5.2.14. Essentially, for all problems affecting the functioning of the System, the Contractor shall own the problem and track it from initiation to closure. For this, the Contractor shall proactively liaise and manage the other service providers of e2i (including the data centre service provider, the facility management service provider, the managed network provider, the system security service provider, and the system monitoring service provider) until the closure of the problem.
- 5.2.15. The Contractor shall ensure that all the Services meet all the service level requirements as prescribed in the Requirement Specifications. In the event that the Contractor fails to meet the stipulated service level requirements as stated in the Requirement Specifications or as otherwise mutually agreed upon (the "Service Levels"). The Contractor shall be liable to e2i for the service

level breaches as set out in Annex 1B-3 Table of Liquidated Damages in Part 1 Section B – Conditions of Contract).

### 5.3. Escalation Process

- 5.3.1. The Contractor shall follow the escalation guidelines specified within NTUC's Quality Management System (QMS) escalation procedure via electronic mail or telephone/SMS. The escalation procedure shall be given to the Contractor upon award of the Contract.
- 5.3.2. For problems under Severity Level '1', the Contractor shall inform e2i immediately through escalation process and shall brief e2i on the causes, area of impact and lead-time for recovery within the Response Time specified in paragraph 5.2.2.
- 5.3.3. The Contractor shall note that the Severity Level of a problem may be escalated based on circumstances such as high impact to user's operations. e2i reserves the right to vary the Severity Level when the need arises.
- 5.3.4. The Contractor shall notify e2i's helpdesk when the System is not available.
- 5.3.5. The Contractor shall escalate any infrastructure problems back to the relevant e2i's helpdesk if the problem is determined to be caused by the infrastructure of the System.
- 5.3.6. The Contractor shall attend meetings with the various e2i's helpdesk managers if there is system instability or whenever there is a need to close the escalation gaps between the Contractor's helpdesk and e2i's helpdesk.
- 5.3.7. The Contractor shall attend meetings initiated by e2i together with e2i's helpdesk to discuss on the major problems or issues encountered by users.

### 5.4. Problem Management System

- 5.4.1. The Contractor shall propose a system ("Problem Management System") to enable its staff to log, update and track the status of the problems and major support activities.
- 5.4.2. Where problems are communicated to the Contractor through e2i's helpdesk or via telephone or electronic mail from e2i user directly, the Contractor is expected to log all such problems reported into the Problem Management System and shall respond to the problem as stipulated in paragraph 5.2.2.
- 5.4.3. The Contractor's helpdesk shall provide incident numbers to the users or e2i's helpdesk who have reported the problems.
- 5.4.4. e2i may from time to time requests the Contractor to locate specific type of problems or helpdesk calls logged by specific users. The Contractor shall be

able to extract and print this information from the Problem Management System.

- 5.4.5. For any problems/defect and resolution, e2i's Representative shall be updated of its status according to the timing specified in paragraph 5.2.2.
- 5.4.6. All problems/defects shall be tracked. There must be proper acknowledgement of all reported System errors and encountered problems and monitoring of the status of the reported errors and problems by the Contractor.
- 5.4.7. The Problem Management System shall be able to capture the following information:
  - (a) caller information (name, department, telephone number, location, email address);
  - (b) date and time of user/ e2i's helpdesk call;
  - (c) type/category/sub-category of problem;
  - (d) problem description;
  - (e) details of problem resolution;
  - (f) date and time of response;
  - (g) date and time of problem resolution;
  - (h) date and time of problem closed; and
  - (i) Severity Level of problem.
- 5.4.8. The Contractor shall also provide an analysis of the problems encountered and propose actions to prevent these problems from recurring and pre-empt similar problems from occurring.
- 5.4.9. The Contractor shall be measured on its performance against the Service Levels for production support, via the Problem Management System.
- 5.4.10. The Problem Management System shall be made available to e2i's Representative as and when needed.

## 5.5. Change Request

- 5.5.1. The Contractor shall propose the form of change request which will detail the impact of changes to the System. Such form shall be approved by e2i before being used for change request purposes during the Contract Period.
- 5.5.2. For each change request, the Contractor shall propose in its proposal ("CR Proposal") the man-days required for such change request and compute the fees payable according to the man-day rates proposed in Annex 1 A - 3 (Price Schedule) of the Tender documents that have been accepted by e2i in its Letter of Acceptance. e2i may exercise the right to engage such services from the Contractor on the basis of such man-day rates and man-days required.

- 5.5.3. Should e2i decide to engage such services from the Contractor, e2i will raise a work order that sets out details of such engagement (“Work Order”) and the Contractor shall undertake to provide such services pursuant to the Work Order.
- 5.5.4. The time taken by the Contractor to perform the impact analysis and resource estimation for the Change Request shall be within five working days. The time taken by the Contractor to provide a Proposal for the Change Request shall be within seven working days, or a duration mutually agreed between the Contractor and e2i.

## 5.6. Service Request

- 5.6.1. SRs which do not warrant changes or enhancements to the source codes/software of the System, the Contractor shall provide such services to the System as part of the Maintenance Services, at no additional cost to e2i. Examples include data extraction required by auditors, data patching due to program bugs or data conversion error, creating of authorisation approval matrix, simple configuration changes that require only verification, creating/updating user profile, creating/updating/deleting/inactivating user accounts and password regeneration requests.

### 5.6.2. Service Request Service Levels

The Contractor shall submit the SR proposal based on the following assessment period:

| Classification | Definition                                                                                                                 | Assessment Period           |
|----------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <b>Minor</b>   | Service Request that requires less than or equal to one (1) working days to complete                                       | Within one (1) working days |
| <b>Medium</b>  | Service Request that requires more than three (3) working days but less than or equal to five (5) working days to complete | Within two (2) working days |

|               |                                                                            |                             |
|---------------|----------------------------------------------------------------------------|-----------------------------|
| <b>Major</b>  | Service Request that requires more than seven (7) working days to complete | Within two (2) working days |
| <b>Urgent</b> | Service Request that is deemed urgent by e2i                               | Within two (2) working days |

Note: The “*Assessment Period*” shall be the time taken by the Contractor to perform the impact analysis and resource estimation for the relevant Service Request

The Contractor shall ensure that all approved Service Requests are completed and implemented based on the following:

| <b>Classification</b> | <b>Time to Complete</b>                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------|
| Minor                 | Within one (1) working days                                                                 |
| Medium                | Within three (3) working days                                                               |
| Major                 | Based on mutual agreement between Contractor and e2i                                        |
| Urgent                | Within three (3) working days or to be based on mutual agreement between Contractor and e2i |

#### 5.7. Training and Knowledge Transfer

- 5.7.1. All training should be conducted on site or in premises to be supplied by e2i.
- 5.7.2. The Contractor should include a full and comprehensive training proposal in its Tender proposal. This should include courses to be conducted, course contents, class size, timetable(s), trainee pre-requisites, duration of each course and instructors’ resume.
- 5.7.3. e2i reserves the right to accept part or all of the training courses and the Contractor may be required to make the necessary amendments to the training courses and training materials wherever necessary.

- 5.7.4. The Contractor shall be responsible for setting up the entire training environment of the System. If needed, the Contractor shall provide all necessary training equipment that are not currently available in e2i for these training purposes.
- 5.7.5. The medium of instruction and training document shall be in English. The Contractor should provide each trainee with a complete set of training documents and materials for his retention.
- 5.7.6. For every course conducted by the Contractor, all training materials (hard and soft copies) should be made available to e2i. e2i should have the right to reproduce and use these training materials to conduct in-house courses for its personnel.
- 5.7.7. The Contractor's responsibilities shall include the preparation of presentation materials, briefings, and any other information. In some cases, the Contractor should provide the materials and assist in conducting the briefing sessions to e2i's senior management and key users.

#### 5.8. Communication Plan

- 5.8.1. The Contractor shall, in consultation with e2i, undertake the responsibility to define and implement appropriate communication plans for the various groups which shall include:
  - (a) general users;
  - (b) senior management;
  - (c) third party vendors; and
  - (d) Sub-contractors.
- 5.8.2. The Contractor shall anticipate possible interfacing issues and undertake to work with and ensure that the third-party vendors are sufficiently briefed on the scope of services and that their roles and responsibilities are clearly defined.
- 5.8.3. The Contractor's responsibilities shall include the preparation of presentation materials, publicity brochures, briefings and any other information. In some cases, the Contractor shall provide the materials and assist in conducting the briefing sessions to e2i's senior management and key users.

#### 5.9. Quality Assurance

- 5.9.1. The Contractor shall conform to the Standards and Procedures in NTUC's Quality Management System (QMS). These shall be provided to the Contractor upon request. Where alternative standards, procedures and methodology are



proposed, the Contractor shall provide details of the alternatives used, state the deviation to NTUC's QMS products and processes. The Contractor shall also explain in detail the quality controls that would be put in place to ensure the quality and maintainability for the delivery System in a Quality Assurance (QA) plan.

- 5.9.2. The Contractor may be required to adopt NTUC's methodologies, standards, and procedures, including those that may be introduced from time to time during the Contract Period should e2i determine that the proposed methodologies, standards and procedures are not satisfactory.

#### 5.10. Documentation

- 5.10.1. The Contractor shall provide all Documentation written in English and expressed in clear, consistent, readily understandable, and defined terms.
- 5.10.2. The Contractor shall supply sufficient Documentation including, but not limited to the following:
- (a) Application Software documentation;
  - (b) user/training guide;
  - (c) document control documentation; and
  - (d) any other documents specified in the Requirement Specifications.
- 5.10.3. e2i reserves the right to reproduce any Documentation supplied with the System for its own internal use.
- 5.10.4. The Contractor shall provide any revised editions, supplementary materials or new publications relevant to the System at no extra cost to e2i.
- 5.10.5. The Contractor shall ensure that proper documentation of the System configurations, the changes made and the reasons or rationale for change are recorded for traceability.
- 5.10.6. The Contractor shall adhere to NTUC's QMS standards for quality records.
- 5.10.7. Documentation shall be managed in NTUC's SharePoint.
- 5.10.8. All documentation formats shall be subjected to approval by e2i.
- 5.10.9. All documents produced by the Contractor in fulfilling this Contract, shall become the property of e2i. e2i reserves the right to reproduce, at no cost whatsoever, any documentation supplied with the System for its own uses. Prior approval must be obtained from e2i for any reproduction and distribution of documents produced by the Contractor.

#### 5.11. Exit Management

- 5.11.1. The Contractor will be given One (1) month before the expiry or termination of the Contract to hand over the existing / remaining Services to a new contractor appointed by e2i. The Contractor should plan the transition accordingly to ensure that it will be completed before the expiry of the Contract. Any additional cost incurred due to the delay in transition caused by the Contractor shall be borne by the Contractor.
  - 5.11.2. The Exit Plan shall include the following activities:
    - (a) Processes and procedures.
    - (b) Roles and responsibilities of the Contractor and e2i.
    - (c) Detailed schedule with clear milestones.
    - (d) Schedule for hand-over of outstanding tasks.
    - (e) Application/Systems documentation which includes but not limited to source code, functional requirements specifications, technical design specifications.
    - (f) Operation manual which includes backup/recovery procedures, start up and shutdown procedures.
    - (g) Security procedures.
  - 5.11.3. The exit transition period shall be managed and supervised by e2i.
  - 5.11.4. The Contractor shall be responsible to conduct a detailed hand-over, inclusive of briefing and training sessions, of the complete system to e2i and the next Contractor. Any cost incurred during the period of hand-over shall be borne by the Contractor. The hand-over shall be conducted concurrently with the on-going support required of the Contractor without affecting the Service Levels.
  - 5.11.5. The Contractor shall hand-over all necessary documentation of the hosting hardware, database and application software and records of problem resolution required for the effective maintenance of the systems.
  - 5.11.6. All user accounts and access rights assigned to the Contractor shall be revoked upon the expiration of the Contract. The revocation shall be carried out in a timely manner.
- 5.12. Quality Assurance and Measurement
- 5.12.1. The Contractor is preferred to be ISO 9001 certified to carry out the Services stated in this Contract.
  - 5.12.2. The Contractor shall conform to the Standards and Procedures in NTUC's Quality Management System (QMS). These shall be provided to the Contractor upon request. Where alternative standards, procedures and methodology is proposed, the Contractor shall provide details of the alternatives used, state the deviation to NTUC's QMS products and processes. The Contractor shall

also explain in detail the quality controls that would be put in place to ensure the quality and maintainability for the delivered System in a Quality Assurance (QA) plan.

- 5.12.3. The Contractor may be required adopt NTUC's methodologies, standards and procedures, including those that may be introduced from time to time during the Contract Period should e2i determine that the proposed methodologies, standards and procedures are not satisfactory.

#### 5.13. Performance Measurement

- 5.13.1. The Contractor shall establish a mechanism to collect, analyse and report its performance against the Service Levels specified by e2i. e2i may from time to time require other measurements.
- 5.13.2. The Contractor shall propose its own working performance indicators and measurements to assure e2i that the Service Levels are met.

#### 5.14. Audit

- 5.14.1. The Contractor shall permit e2i to conduct such audit or other inspection of Services provided to e2i, as e2i deems necessary. Such inspection shall also include the examination of any materials, documents, equipment, premises and facilities relating to the Services provided under this Contract that are within the possession, custody or control of the Contractor. e2i shall inform the Contractor in advance for any inspections and the Contractor shall ensure that such inspections shall not affect the Service Levels. The right of audit may be extended to the Contractor's subcontractors who are involved in the project.
- 5.14.2. The Contractor shall provide the resources necessary to work with e2i's appointed auditors to assist in the audit and its review at no additional cost to e2i.
- 5.14.3. The Contractor shall implement the audit recommendations and provide evidence for the audit recommendations carried out, to e2i not later than one (1) calendar month after e2i's approval of the audit report.
- 5.14.4. The Contractor shall propose follow-up plans to address audit findings, subject to e2i's approval. The proposal shall include a schedule of the closure of audit findings, subject to mutual agreement.
- 5.14.5. The Contractor shall monitor and ensure that corrective follow-up actions are carried out for the audit findings. The Contractor shall provide evidence, for the corrective follow-up actions carried out, to e2i no later than one (1) calendar month after e2i's approval of the audit report.

- 5.14.6. The implementation of the audits recommendations and corrections shall be done at no additional cost to e2i if the audit gaps are due to the Contractor's failure to meet the Requirements Specifications.

## **6. TECHNICAL REQUIREMENTS**

### **6.1. Objective**

- 6.1.1. The Contractor shall ensure that the System meets the technical requirements stated in this section.
- 6.1.2. Additional information regarding the relevant technology tools, software stack, and cloud deployment architecture shall be shared with the Vendors upon request.

### **6.2. User Interface**

- 6.2.1. The user interfaces shall be web-based and mobile responsive.
- 6.2.2. All public-facing user interfaces shall integrate with Google Analytics or equivalent to capture sufficient data for user experience related analytics

### **6.3. Sign in**

- 6.3.1. e2i staff and other relevant users shall sign in via NTUC's identity management platform. Integration with NTUC's identity management platform shall be via OIDC or SAML 2.0.
- 6.3.2. Members of public shall sign in via NTUC's Public Login Service. NTUC's Public Login Service is an authentication service built on the OpenID Connect (OIDC) authentication protocol.
- 6.3.3. Companies shall sign in via government-approved corporate digital identity systems such as Corppass.
- 6.3.4. All privileged/admin e2i users shall authenticate using at least two forms of verification (e.g., password + OTP, biometrics) for access to the system.
- 6.3.5. The Contractor shall implement robust access controls and authentication mechanisms to safeguard NTUC's systems, networks, and data from unauthorised access.

### **6.4. Log out for non-active users**

- 6.4.1. The System shall automatically log out users after a period of inactivity and secure session handling (e.g., HttpOnly, Secure flags on cookies) should be implemented.
- 6.4.2. The System shall be designed such that the inactivity log out period is configurable.

### **6.5. Application Design**

- 6.5.1. The System shall be designed to be modular and extensible to cater for future growth and changes while localising the changes required.

- 6.5.2. The System shall be designed to ensure that common codes are reused where possible instead of duplicating these codes.
  - 6.5.3. The System shall not contain any hidden functionalities that e2i is not aware of.
  - 6.5.4. The System shall not hard-code any parameters (e.g., IP address, port number, path, file location, host name, domain name, etc.). The system shall ensure that passwords, cryptographic keys, secrets etc. are not exposed in code or configuration files.
  - 6.5.5. The System should be designed leveraging on a data dictionary, so that data is maintained and referenced in a consistent and transparent manner within the System. Examples of such design considerations include business rules or constraints applied to the data, check constraints, as well as referential integrity rules.
  - 6.5.6. Data dictionary documentation shall indicate the fields containing personal data.
- 6.6. Generative AI-based Summary / Recommendation Engines
- 6.6.1. The Artificial Intelligence (AI) summary/recommendation engines should consider, at the outset.
  - 6.6.2. Protection of personal data.
  - 6.6.3. Explainability of the summaries/recommendations, e.g., enabling the end-users to see relevant prompts and citations in the responses.
  - 6.6.4. Enabling the end-user to see the engine's level of confidence in its responses.
  - 6.6.5. Feedback loops to enable continual improvement of the recommendations.
  - 6.6.6. Flexibility in using an ensemble of language models for different tasks or even within a single task.
  - 6.6.7. Responsible AI safeguards to prevent generation of harmful, biased, and unethical outputs.
- 6.7. Authorisation Design Guidelines
- 6.7.1. The Contractor shall work with e2i to setup an authorisation matrix for Access Roles segregation, after studying e2i's key business processes and requirements. The authorization matrix shall define roles and responsibilities and assign proper access to each user of the System and the Contractor shall work with various stakeholders to define and confirm the authorization matrix.
  - 6.7.2. Users should be assigned to User Groups with authorisation assigned at the User Group level where possible.
- 6.8. Up-To-Date Technology

- 6.8.1. The Contractor shall ensure that the technical design of the System and the platform on which it operates, harness up-to-date technologies.
  - 6.8.2. In the event of a newer version of the Base Software or related products/technology released before the stipulated commissioning date and the version is different from the proposed version in Contractor's Tender, the Contractor shall assess the impact and propose the most suitable version to be adopted for production release with strong justification. Throughout the term of the Contract, the Contractor shall ensure that the version of the Base Software and related products/technologies remain under active vendor maintenance and support, including timely release of security patches and updates to address known vulnerabilities. The Contractor shall ensure the deployed versions shall not be more than 2 major versions behind the latest generally available release. Any deviation from this requirement must be risk assessed, documented and mutually agreed between the Contractor and e2i.
  - 6.8.3. The Contractor shall not propose any obsolete technologies to be used in the System. Should there be a need to introduce such technologies, this shall be mutually agreed between the Contractor and e2i. An upgrade path shall also be described in the proposal. The Contractor shall perform, at least annually, a formal review of the Base Software and all related products/technologies to ensure they remain under active vendor maintenance and support. The review shall verify continued availability of security patches and updates to address known vulnerabilities throughout the contract period, and any identified risks shall be documented and managed in accordance with the risk management process.
  - 6.8.4. The Contractor shall conduct regular risk assessments and implement risk management practices to identify, assess, mitigate, and monitor cybersecurity risks throughout the contract period.
  - 6.8.5. The Contractor shall promptly update and upgrade cybersecurity measures as necessary to address emerging threats, vulnerabilities, and changes in regulatory requirements during the contract term.
  - 6.8.6. The Contractor shall ensure all components, including web servers, application libraries, and third-party services to be kept up-to-date with the latest security patches.
- 6.9. Ease of Operation
- 6.9.1. The Contractor shall design the System to, where possible and applicable, automate complex job processes, reduce the number of tasks for a process, etc. The Contractor shall ensure that the System is simple to use with clear layout and usage of simple terms.

- 6.9.2. The Contractor shall design the System with the principles of user-friendliness and simplicity such that operating the System will not be cost-intensive, cumbersome and time consuming. The Contractor shall ensure that the design of System shall facilitate timely and accurate presentation of relevant information.
- 6.9.3. The Contractor shall design the System to provide e2i's authorised personnel with the feature to schedule, monitor, and reconcile the backend bulk processes (if any).
- 6.10. System Interface
  - 6.10.1. The System Interfaces shall follow the relevant NTUC policies, guidelines, and conventions.
  - 6.10.2. The Contractor shall provide the implementation services for the delivery of the System interfaces based on the Requirement Specifications.
  - 6.10.3. The Contractor shall design system interfaces that are robust, scalable, and extensible.
  - 6.10.4. Bulk data transfers are preferred to happen over secure file transfer or secure object storage services.
  - 6.10.5. Incoming synchronous calls to the System are preferred to be implemented as secured REST APIs and routed via NTUC's API Management Gateway.
  - 6.10.6. Incoming asynchronous calls to the System are preferred to be implemented using a secure enterprise messaging service.
- 6.11. Exception handling
  - 6.11.1. The System shall provide necessary error handling for ease of troubleshooting, prevention of information leakage, and management of the users' experience.
  - 6.11.2. All user inputs shall be validated at both the client-side and server-side to prevent injection attacks such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). Error messages shall be generic and not reveal sensitive information (e.g., stack traces, database details) that could aid an attacker.
  - 6.11.3. Error messages displayed to users should be easily understood without divulging unnecessary information and advise the users on possible next steps.
  - 6.11.4. Error logs shall capture sufficient information to enable troubleshooting and root cause analysis.
  - 6.11.5. Error logs shall be piped to NTUC's Application Monitoring Service where applicable.
  - 6.11.6. A hierarchy of error levels, codes, and messages should be developed for each application modules.



- 6.11.7. There should be error codes corresponding to error messages so that it is easier to modify the messages without code modification.

#### 6.12. Application Audit

- 6.12.1. The System shall be able to capture audit trails of selected “create”, “update” and “delete” transactions performed through the Administrative module.
- 6.12.2. The information to be logged includes the user identifiers such as user ID and machine name (where possible), the action taken and the date and time stamp of these transactions.
- 6.12.3. The System shall capture audit information on any unauthorised access of data in the System, or to System functions.
- 6.12.4. The System shall allow only authorised e2i users to view the audit information.
- 6.12.5. The System shall ensure that these audit trails be protected from being modified including Privileged Users.
- 6.12.6. The System shall have the facility to store the audit information online for varying periods depending on the type of audit trails before they are archived. The general guideline would be one (1) month online for database audit trail and three (3) months online for other audit trails.

#### 6.13. Subcontractor and Third-Party Compliance

- 6.13.1. The Contractor shall ensure that all subcontractors and third parties involved in the performance of services under this contract adhere to cybersecurity requirements equivalent to those stated herein.

#### 6.14. System Performance and Load Testing

- 6.14.1. The System shall support a system load of 20 concurrent users for staff access.
- 6.14.2. The System shall also support a system load of 20 concurrent users for access by members of the public when commissioned. The System shall be scaled to support up to 100 concurrent users for access by members of the public.
- 6.14.3. The concurrency for staff users and members of the public applies to the relevant components of the solution and is cumulative for components used by both sets of users.
- 6.14.4. The System is deemed to be able to support the concurrent load if the 90-percentile response time is less than 3 seconds. For very complex and longer running transactions, alternative response timings may be proposed.
- 6.14.5. The proposal shall include the performance testing approach.
- 6.14.6. An independent 3rd party shall conduct the required performance tests.

#### 6.15. System Availability

- 6.15.1. The monthly System Availability shall be 99.5% or better. The System Availability Level is defined as:

$$\frac{\text{Actual Total System Uptime}}{\text{Planned Total System Uptime}} \times 100\%$$

- 6.15.2. “Actual Total System Uptime” is the Planned Total System Uptime less Unscheduled System Downtime.
- 6.15.3. “Planned Total System Uptime” is the number of operating hours in the relevant month less Scheduled System Downtime.
- 6.15.4. “Scheduled System Downtime” is the number of hours in relevant month where the System is unavailable due to scheduled maintenance approved by e2i in writing.
- 6.15.5. “Unscheduled System Downtime” is the number of hours in the relevant month where the System is unavailable due to reasons other than scheduled maintenance approved by e2i in writing.

6.16. Backup and Disaster Recovery

- 6.16.1. Regular backups of data must be performed, and a disaster recovery plan should be in place to ensure business continuity in the event of a breach or failure.

6.17. Technical Documentation

- 6.17.1. The Contractor shall provide comprehensive technical documentation that should include the following where relevant:
- (a) Cloud Service Provider(s) for hosting the System - including details of the cloud infrastructure, region, availability zones etc.
  - (b) Solution Architecture Overview: High level descriptions and diagrams illustrating the overall architecture of the System outlining key components, services, external interfaces and their interactions.
  - (c) Application Architecture: Detailed descriptions and diagrams illustrating the application components, external interfaces and their interactions.
  - (d) Technical Architecture: Details of data sources and interfaces with external systems, including a detailed technical architecture diagram.
  - (e) Data Architecture: Details of the overall design and structure of data of the System. This includes data models (such as entity-relationship

diagrams), data dictionaries, data integration as well as data security measures.

- (f) Security Architecture: Description of the security architecture, including authentication mechanisms, access controls, encryption methods, and data protection measures implemented to safeguard the system and user data.
- (g) Technology Stack: Details of the technology stack used in the development and deployment of the System, including programming languages, frameworks, libraries, and third-party services.
- (h) Scalability and Performance: Specifications for scalability measures implemented to accommodate increasing user loads and transaction volumes.
- (i) Operations: Define and document the operational procedures for the proposed application and any cloud services they depend on.

## 6.18. Infrastructure

### 6.18.1. Hosting, Deployment and Technology Stack

- (a) The System shall be hosted in NTUC's cloud environment and follow the relevant NTUC's policies, guidelines, and conventions.
- (b) The proposal shall include the number of environments required in NTUC's cloud environment in each Stage to properly support the System lifecycle.
- (c) Deployment into NTUC 's cloud environments is preferred, with at least one environment configured for zone redundancy.
- (d) Use of native cloud services and modern frameworks (e.g., .NET) is preferred where feasible
- (e) For systems hosted within the NTUC cloud landing zones, the Contractor shall provide a detailed inventory of the cloud resources required by the proposed solution, including the respective resource types, sizes or SKUs, and the estimated monthly cloud costs based on the proposed configuration.
- (f) The contractor shall utilize the NTUC's DevOps platform and infrastructure-as-code tools where applicable.
- (g) All relevant source code shall be stored in the NTUC's version control repository.
- (h) All production artifacts shall be built from NTUC's DevOps repository.

- (i) Automated build, test, and deployment pipelines are required (where possible). The proposal shall include details on the build, test, and deployment approach.
- (j) Keys, secrets, and credentials must be securely generated and stored using a secure key management service. Access must be strictly controlled and limited to authorized personnel.
- (k) The system shall integrate with a cloud-native monitoring and telemetry service.
- (l) All sensitive data (including user credentials and personal information) must be encrypted both in transit (using TLS 1.2 or higher) and at rest (using AES-256 or equivalent encryption).
- (m) Data Masking: For sensitive information displayed in user interfaces, appropriate data masking techniques should be employed (e.g. displaying only the last four digits of a credit card number).
- (n) Regardless of the above preferences, Contractor shall propose the solution's technology stack and deployment that best meets all the requirements and provide justifications as necessary.

**6.18.2. Data Residency for Personal Data:**

- (a) All Personal Data is to be hosted in Singapore. Personal Data shall not be transferred outside Singapore or be accessed by parties outside Singapore.
- (b) Should data be hosted outside of Singapore, the contractor shall indicate in their proposal the location where the data resides.
- (c) Data Retention and Deletion: The Vendor shall define data retention policies outlining the duration for retaining customer data. Upon contract termination or request from e2i, the Vendor shall securely and permanently delete all customer data from its systems.
- (d) The Vendor shall define and propose (as an option) a data export solution to export business data on a periodic basis (e.g. quarterly, monthly) to e2i's approved cloud tenancy via secure transfer or other mutually agreed mechanisms.

**6.19. Security Measures**

- 6.19.1. The System shall be implemented to include the following security measures:
- 6.19.2. Use of cloud native network firewalls, web application firewalls or equivalent as required by NTUC policies, guidelines, and conventions.
- 6.19.3. The system shall be protected by a properly configured Web Application Firewall (WAF) to mitigate common web-based attacks. WAF rules shall be securely configured and optimised to minimise exceptions. Any exceptions

shall be limited, justified, documented, and approved through formal risk management and change control processes.

- 6.19.4. The Contractor shall ensure that all required network connectivity for the system is formally documented, including source and destination details, ports, protocols, and data flow justifications. All firewall rules shall be subject to prior review, risk assessment, and approval through the established change management process. Periodic reviews shall be conducted to validate the continued necessity of such connectivity, and any unused or unnecessary rules shall be promptly removed.
- 6.19.5. Use of cloud security detection tools or equivalent as required by NTUC policies, guidelines, and conventions.
- 6.19.6. Use of cloud native logs or equivalent as required by NTUC policies, guidelines, and conventions.
- 6.19.7. Automated notifications when suspicious activities are detected.
- 6.19.8. Ensure logs are streamed to designated endpoints such as monitoring and security platforms.
- 6.19.9. Log all access to personal data.
- 6.19.10. Encrypt data at rest and in transit in accordance with NTUC policies, guidelines, and conventions.
- 6.19.11. Put in place access controls following the principle of least privileges and ensure that access is only given to authorized users.
- 6.19.12. The contractor shall integrate with NTUC's existing secure file upload mechanisms (if applicable).
- 6.19.13. The Contractor shall perform quarterly Vulnerability Assessment and annual Penetration Testing (VAPT) on System and fix all necessary issues according to NTUC policies, guidelines, and conventions before going live.
- 6.19.14. The Contractor shall comply with all of NTUC's policies and procedures, including the NTUC IT Policy and Cybersecurity Governance and Escalation Framework.
- 6.19.15. The Contractor shall utilise NTUC's existing Privileged Access Management ("PAM") solution currently in place for all relevant activities. The System developed by the Contractor shall be designed and implemented to seamlessly integrate with the existing PAM environment, ensuring secure, interoperable, and policy-compliant access controls in accordance with established PAM processes.
- 6.19.16. The Contractor shall adhere to recognized cybersecurity standards and frameworks, including but not limited to ISO/IEC 27001, NIST Cybersecurity Framework, or equivalent standards deemed appropriate by NTUC.

## 6.20. Certifications

6.20.1. The contractor shall provide relevant certifications achieved for Software-as-a-Service (SaaS) solutions if proposed. Examples of such certifications are listed below:

- (a) ISO/IEC 27001 – Internationally recognised standard for information security management systems (ISMS). Conformity with ISO/IEC 27001 means that an organization has put in place a system to manage risks related to data security, following best practices of this International Standard (applicable to organisations in general).
- (b) SOC 2 – Trust Services Criteria – Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy (applicable to organisations in general).
- (c) PCI-DSS – Payment Card Industry Data Security Standards to handle credit card data (applicable mainly to payment providers).
- (d) Cloud Security Alliance (CSA) STAR – CSA STAR Level 1 (self-assessment) and Level 2 (third-party certification) build on ISO/IEC 27001 and SOC2, providing security assurance for cloud services. Contractors should indicate which cloud their services are built on, and whether the cloud provider has a CSA STAR level.

## ANNEX A: PAYMENT MILESTONES

| Grant Management System Tender - Payment Milestone Schedule<br>(excluding maintenance contract cost) |                                        |                                                                                                                                                |          |                                                                                                  |
|------------------------------------------------------------------------------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------|
| Milestone ID                                                                                         | Milestone Name & Phase                 | Key Deliverables                                                                                                                               | Payout % | Target Criteria / Definition of Done                                                             |
| <b>MS-01</b>                                                                                         | Project Award & Mobilization           | Kickoff meeting completed, project charter signed, and initial development/staging environment provisioning completed.                         | 10.0%    | Clears initial resource mobilization costs for the vendor.                                       |
| <b>MS-02</b>                                                                                         | Discovery & Design Sign-off            | Completion and approval of Business Requirements Document (BRD), UI/UX wireframes, and high-level system architecture design.                  | 15.0%    | Approved architectural designs and signed-off user journeys.                                     |
| <b>MS-03</b>                                                                                         | Core Build                             | Core backend architecture, database schemas, and critical user authentication modules built and deployed to staging environment.               | 20.0%    | Demonstration of core foundational functionality working stably in staging.                      |
| <b>MS-04</b>                                                                                         | Integration, Features & Data Migration | Frontend integration, core functional features, and third-party API configurations fully developed and compiled.                               | 20.0%    | Internal QA passed successfully; system ready for formal User Acceptance Testing (UAT).          |
| <b>MS-05</b>                                                                                         | Testing & UAT Sign-off                 | Successful completion of UAT by client stakeholders, remediation of security/penetration testing vulnerabilities, and data migration dry runs. | 15.0%    | Formal client sign-off achieved with zero 'Critical' or 'High' defects remaining in the UAT log. |
| <b>MS-06</b>                                                                                         | Go-Live & Production Deployment        | Platform is live in the production environment, accessible to end-users, and technical operations/handover                                     | 10.0%    | Successful production cutover window and verified platform                                       |

|                               |                            |                                                                                                           |               |                                                                                                       |
|-------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------|
|                               |                            | documentation completed.                                                                                  |               | stability for the first 48 hours.                                                                     |
| <b>MS-07</b>                  | Post-Go-Live PGP Retention | Upon completion of post-launch stabilization support, monitoring, and priority bug fixing ('PGP Period'). | 10.0%         | Milestone released only after the stabilization period concludes with standard SLA metrics fully met. |
| <b>Total (Implementation)</b> |                            |                                                                                                           | <b>100.0%</b> |                                                                                                       |

- Definition of Done (DoD). No milestone payment shall be triggered purely by elapsed calendar time. Every milestone requires a formal sign-off artifact (e.g., architectural sign-off document, UAT certificate signed by the Project Sponsor) verifying that all criteria have been met.
- Defect Thresholds. For the UAT sign-off (MS-05), a strict threshold of zero 'Critical' or 'High' severity defects must be maintained. Any such open defects automatically stop the milestone completion until fixed, retested, and verified.
- PGP Retention. The final 10% payment (MS-07) to ensure the contractor provides robust support during operational rollout and does not divert resources post-deployment. Released only upon successful completion of the stabilization window.
- (3 + 1 + 1) Maintenance fees shall be invoiced and paid quarterly in arrears. The Contractor shall submit quarterly invoices supported by service reports, SLA achievement reports, incident logs and other evidence reasonably required by e2i to verify satisfactory delivery of Maintenance Services. Payment shall be subject to e2i's acceptance of the services performed during the relevant quarter. e2i reserves the right to withhold payment, in whole or in part, where service levels have not been achieved, contractual obligations remain outstanding, or supporting evidence is incomplete. No advance payment shall be payable unless otherwise approved by e2i in writing.