USAID CATALYZE

Requirements Specification Report for the Management Information System (MIS)

July 22, 2021

Project Data Sheet	
Funder	United States Agency for International Development (USAID)
Reporting Office	N/A
Country	N/A
Activity Name	Requirements Specification for USAID CATALYZE MEL MIS
Prime Managing Contractor	Palladium International LLC
Partners	[redacted]
Responsible Official	
Doc Number	MIS01
Version	1.0
Effective Date	June 22, 2021
AOR/COR/Activity Manager Name & Office:	[redacted]
Approved By	
Summary of Changes	Incorporated initial feedback into this version (1.o)
Geographic Focus:	Worldwide

Statement:

This is a controlled document. Any printed documents become uncontrolled.

Table of Contents

1. Purpose

This document provides the list of requirements, functional and technical, for the USAID CATALYZE Management Information System to support MEL data collection, storage, retrieval, sharing, and analysis needs (MEL MIS). This system will be the central repository of the MEL data for all the USAID CATALYZE Buy-ins. Buy-in MEL leads and implementing partners' MEL team will use the system to store MEL data in a timely manner. Palladium MEL, Communications and other teams involved in the USAID CATALYZE project along with the USAID team, will use the MIS to view MEL data and track the performance of the program and Buy-ins.

2. Applicability

This plan is applicable to the USAID CATALYZE program MEL data collection, performance monitoring and tracking, and reporting at the portfolio- and Buy-in level. Any deviation from this plan requires the approval of the Responsible USAID CATALYZE MEL lead.

The USAID CATALYZE program team has in place Policies, Standard Operating Procedures (SOPs), Business Processes, and Tools to support implementation of this internal project, which has as its primary aim to guide Palladium's procurement of a MEL MIS.

3. Definitions

"Buy-in" - Individual multi-year projects in multiple geographies addressing a wide array of development challenges, which are implemented in response to a need identified by a client USAID Mission, Operating Unit (OU), or Independent Office (IO)

"Implementing Partner" - Organizations that subcontract or grant awardees in order to implement the design and/or implement work plans approved by USAID USAID CATALYZE to support centrally funded (CLIN1) or Buy-ins (CLIN2) activities.

"MEL Team" – Palladium HQ MEL Team, composed of the Senior M&E Manager and the MEL partner.

"USAID COR" – The USAID Contracting Officer Representative on the USAID CATALYZE project.

"AMU" – Activity Management Units at Palladium responsible for the management of implementation for each Buy-in.

"Business Process" - A sequence of linked tasks and related decisions that result in or contribute to the delivery of a product or service.

"Company" - Refers to Palladium Group Holdings Pty Ltd and all of its subsidiaries or related companies.

"Data verification" - A way of ensuring the user types in what they intend, in other words, to make sure the user does not make a mistake when inputting data.

"Data Validation" - Checking the data entered to ensure it conforms with the data requirements of the system to avoid data errors.

"Guidelines" - The written elaborations on Company policy that provide further information and interpretation for the implementation of policy.

"Logical Framework" - A table that lists your program activities, short term outputs, medium term outcomes, and long term goals meant to show the logic of how the activities will lead to the outputs, which in turn lead to the outcomes, and ultimately the goal.

"Milestone" - The key programmatic and financial targets that the Grantee must meet to qualify for initial or subsequent Grant disbursements (whether in advance of expenditure or reimbursement of funds). Milestones also help measure how a project is progressing towards its ultimate goal of creating change(s).

"MSME" - Micro, Small and Medium Enterprises participating in the USAID CATALYZE program.

"GDPR" - General Data Protection Regulation European Union Law.

4. Overview

CATALYZE's MEL subcontractor has conducted a comprehensive Requirements Assessment, including functional, security and technical requirements for an integrated MIS for USAID CATALZYE's Monitoring, Evaluation and Learning (MEL), and Knowledge Management (KM) workstreams. Specifically, the Requirements Assessment addresses all current and future requirements and priorities of information collection, analysis, access, security, storage, and sharing. It articulates a data management approach, supporting processes to operationalize this approach, identifies requirements for a system, including a global information system, and recommends possible technology solutions while taking into account functionality, cost (capital and operational expenditure), and timeline to deploy and maintain the systems. In light of this Requirement Assessment, Palladium will procure, host, and manage the actual system.

General Information

4.1. Background

The purpose of USAID CATALYZE, a $250 million, eight-year contract (five-year base period, with a single three-year option period), which uses a facilitated partnership model, is to

craft solutions to crowd in $2 billion in private capital through blended finance (i.e., blended concessional and commercial finance) to USAID partner countries and initiatives.

USAID CATALYZE is structured so that there is a group of core services across the mechanism (referred to as CLIN 1), which both supports and draws from a series of discrete Buy-ins (i.e., individual multi-year projects in multiple geographies addressing a wide array of development challenges, referred to as CLIN 2). The core services contain five 'buckets', i.e. 1) Monitoring Evaluation and Learning; 2) Communications / Knowledge Management / External Relations / Community of Practice; 3) Tool Incubation and Deployment; 4) Buy-in Pipeline Development; and 5) Agency Modalities Enhancement/Facilitator Model Execution.

Learning is a critical pillar of USAID CATALYZE. Given its global nature, USAID CATALYZE has the potential to generate evidence and insights that have the potential to have far-reaching influence on how USAID engages the private sector in development.

For each Buy-in, an Activity Monitoring, Evaluation, and Learning Plan (AMELP) was developed. The AMELP identifies the strategic objectives, data, indicators, outputs, and outcomes that inform and drive each Buy-in activity's monitoring, evaluation, and learning (MEL) over the life of activity (LOA) efforts. The AMELP serves as a framework to support activity management and guide monitoring, evaluation, and learning intended to inform whether and how an activity is progressing toward stated results. Appendix A lists the seven Buy-ins in the Program to date and the geographical regions covered in each Buy-in.

4.2. Objectives

USAID CATALYZE will utilize a MEL MIS that will be developed based on requirements for data collection, analysis, access, and storage. This system, which will utilize web and mobile interfaces and cloud-based hosting and storage, will efficiently handle large amounts of decentralized data. It also will provide state-of-the-art data accessibility, security, storage, and will be customized for USAID CATALYZE's needs. The MEL MIS will consist of a data repository and analytics engine. Both open source (e.g., DHIS2, MYSQL) and configurable commercially available off-the-shelf software (e.g., AirTable, DevResults, Synergy) will be considered for the data repository, and data analytics will either be integrated or handled by external solutions.

The overall objective of the MEL MIS is to ensure that all MEL data for the USAID CATALYZE system from the all Buy-ins is captured in one centralized secure location. The MEL MIS will contain timely MEL data updated on a regular basis with data from the activities in each Buy-in. The system shall be used by the various stakeholders involved in USAID CATALYZE to serve multiple functions and needs. For the Palladium Buy-in Leads, the MEL MIS will be used as their M&E system; for implementing partners, they will upload their MEL data in the MIS on a regular basis. For the USAID CATALYZE M&E team, the system will be used to track indicators and the performance of the various Buy-ins and their respective activities. For Palladium USAID CATALYZE management, USAID and other stakeholders, the system will serve as a reporting platform to view the performance of the program, reports and produce ad-hoc reports as needed.

The USAID CATALYZE program operates in multiple regions and countries within each region including but not limited to Ethiopia, Niger, Burkina Faso, Zambia, Democratic Republic of Congo, South Africa, Peru and Bosnia. As such, the system should have the capability to operate in challenging infrastructure conditions and offer mobile and offline capabilities. Additionally, the system will address the security and access requirements necessary to safeguard the data collected and stored in the system. Some of this data may contain sensitive data such as locality of the activities and the entities engaged in the program.

4.3. Business Drivers

The business drivers for having a centralized repository for the USAID CATALYZE MEL data are many. The main purpose is to have a central repository for all the MEL data enabling the USAID CATALYZE MEL team and leadership to track the performance of all the USAID CATALYZE Buy-in from one central dashboard/portal. The second reason is to have a standard process to ensure data quality and timeliness of the data being reported. All data will be reported based on an agreed upon process for data quality checks and "lookup values" across the Buy-ins. This provides standard metrics when comparing performance of similar activities across multiple Buy-ins. Furthermore, a centralized repository removes the need to develop additional processes to aggregate data across the multiple Buy-ins to track global program wide indicators and reporting.

With a centralized system, the MEL team will ensure the security and integrity of the data by i) implementing the required security controls for USAID responsible data framework, GDPR, and other privacy and security compliance requirements; ii) users' access to the data will be controlled and limited to the necessary access for them to perform their daily and program required tasks; iii) data quality processes are performed on a regular basis to ensure accuracy of the data reported and stored; and lastly iv) any future changes in requirements – security, privacy and other regulatory policies, or functional are implemented in one platform and upon rollout will ensure that all Buy-ins remain compliant with these requirements and have access to new functionality.

4.4. Key Stakeholders & User Groups

The set of users who will be using the system are grouped in different groups based on their role in the USAID CATALYZE program and their access requirements. There are four main categories of stakeholders – Primary User, MEL User, Reporting and Viewer, and lastly the Operations group.

The Primary Users are the set of stakeholders who are the implementers of the Buy-ins and overall USAID CATALYZE activities (e.g., Communications) of the program. These are the users who oversee the activities, define the data collection processes, oversee data collection and ensure that the data collected is correct, accurate and timely. These can be the Palladium MEL leads for each Buy-in or the MEL leads of the implementing partners working with Palladium.

The MEL User category consists of the USAID CATALYZE HQ MEL team. These users will define the indicators in the system – both at each Buy-in level nd global program level

indicators – and use the system to review the MEL data to track the performance against indicators of the program at the Buy-in and global program level.

The third category of users are the **Reporting and Viewer** users. These users will use the system to view indicator performance for the Buy-ins and across the program. They will generate predefined and ad-hoc reports and have limited read-only access to the data in the system.

The last group, the **Operations** group, consists of the IT operations team and the group responsible for the maintenance and security of the system including the upgrade of the system when required. The users in this last group are not consumers of any of the data in the system. Their main role is the operational and security monitoring of the system, minimizing downtime and making the system available 24x7x365 to all other stakeholders.

The categories for the stakeholders shall be implemented as roles in the MIS with varying access level based on the interest definition for each category (see Security/Access control requirements in the security requirements, section 8.2).

Table 1 below lists each stakeholder, the group/category they belong to, and their main interest in the USAID CATALYZE MEL MIS.

Table 1- List of stakeholders of the USAID CATALYZE MEL MIS

Key Stakeholder/User Group	Role	Interest
MEL Leads for each Buy-in	Primary User	Advanced easy to use MEL MIS – central location for data repository.
Implementing Partners	Primary User	More accurate approach to submitting data to the USAID CATALYZE MEL team.
USAID CoR	Reporting & Viewer	Accurate and timely reporting of MEL data. Direct access to data for reporting and analysis purposes.
USAID CATALYZE Communications	Reporting & Viewer	Accurate and timely reporting of MEL data. Direct access to data for reporting and analysis purposes.
MEL at HQ (MG & Shahzad)	Reporting & Viewer	Accurate and timely reporting of MEL data. Direct access to data for reporting and analysis purposes. Central location for all the USAID CATALYZE MEL indicators and MEL data.
Knowledge Management (*pending final decision)*	Reporting & Viewer	Capture, distribute, and effectively use knowledge generated across the Buy-ins and at the portfolio-level.
USAID Mission(s)	Reporting & Viewer	Accurate and timely reporting of MEL data. Direct access to data for reporting and analysis purposes.
USAID CATALYZE IT	Operations	Maintenance of the MIS.

5. Business Process Overview

The business process for the MEL MIS is designed to ensure the MEL data is captured in the system in a timely manner following accurate processes with data quality checks in place to ensure the integrity of the data. Each Buy-in collects data of the activities they perform and the beneficiaries engaged in these activities. The MEL MIS updates all Buy-in and USAID CATALYZE level indicators based on the data entered and all the indicators that feed from these data elements using each respective indicator formula.

The main interface to the MEL MIS from all the Buy-ins are the MEL leads, whether Palladium or that of the Implementing Partner. It is the responsibility of the MEL leads to verify that the data has been entered correctly in the system by their team members. The USAID CATALYZE HQ MEL team validates the data periodically for all the Buy-ins. Data is entered in the system on an agreed upon schedule. The MEL MIS shall implement its own business rules to verify the data being entered and flag any errors in an interactive real-time fashion to the system user. Collected data is entered in the system using multiple methods: direct data entry through the use of the system (survey module of the system), or integrated data collection tools/mechanisms such as survey tools (e.g. KoBo, ODK, etc.); data is collected using paper-based data collection and then keyed-in the system; and the third method is the batch upload of data through an API or a provided data upload client interface to the system. Regardless of the data entry method, the system shall implement the same business rules and security measures to validate all the data. Depending on the method used, users will be informed of any data errors/inconsistencies, correct the errors and repeat the data entry/upload process.

As mentioned above, automated indicators are populated when data is entered and verified. Manually populated indicators are updated by the MEL leads from the different Buy-ins. There will be a number of pre-defined reports, report templates, and dashboards. These will be updated with the latest entered data and updated indicators. Users of the system will be able to generate ad-hoc reports using the latest data in the system.

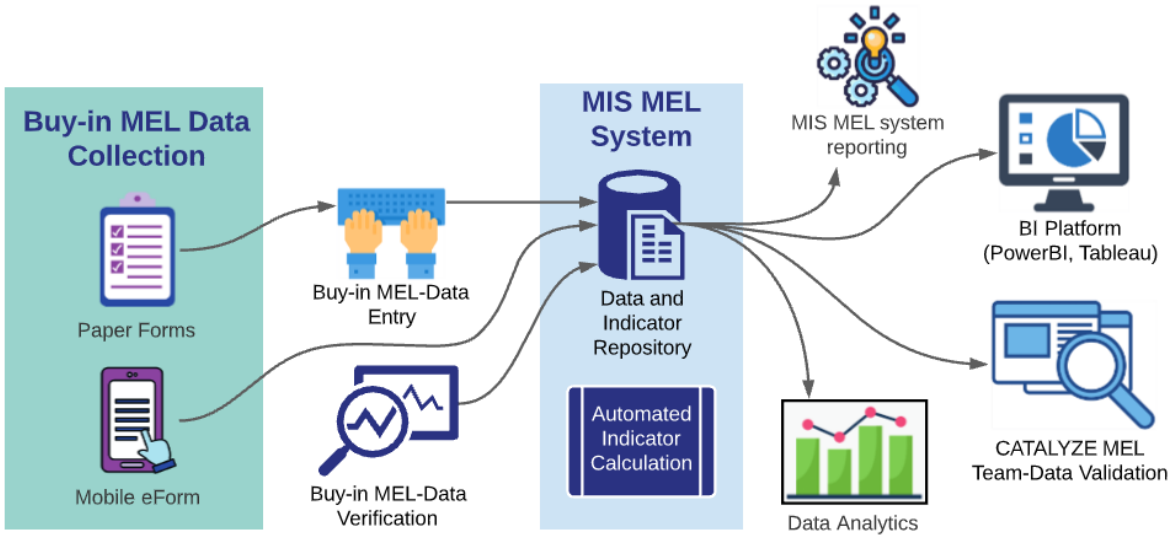
The system shall have in place the ability to control access to the various features, data elements and indicators based on a user's role and the privileges assigned to the role. For example, a Buy-in MEL lead must only have access to the data and indicators that pertain to their Buy-in. They must not have the ability to view nor update data and indicators from other Buy-ins. The USAID CATALYZE HQ MEL Team shall have complete access to the data and indicators for all Buy-ins and USAID CATALYZE wide indicators. Certain operations must be controlled and shall not be executed without the approval from the entities defined. The system must have the ability to allow for changes and approval request workflow processes.

6. USAID CATALYZE MEL MIS Data flow

The USAID CATALYZE MEL MIS will be used by the USAID CATALYZE HQ MEL team, the Buy-in M&E teams and the implementing partners. Some of the Buy-ins will use the system as their MEL MIS systems and others have their own MEL system and will later upload their Buy-in MEL data in the USAID CATALYZE MIS. This ensures the MEL MIS as the central data

repository for all of the USAID CATALYZE MEL data – beneficiary, survey and activity data collected from the Buy-ins and indicator data populated within the MIS from the data collected. In both scenarios, the USAID CATALYZE HQ MEL team performs periodic data validation to ensure the quality and accuracy of the data. Figures 1 and 2 below show the data flows for the two scenarios.

Figure 1 - USAID CATALYZE MEL MIS used as Buy-in M&E

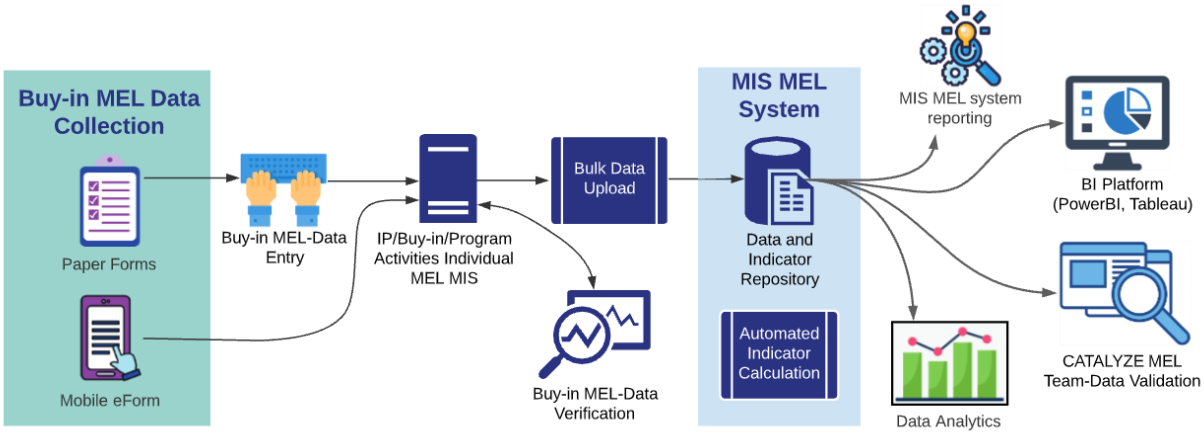


Under scenario 1, in Figure 1 above, where the Buy-ins use the MEL MIS as their M&E system, data is collected by the Buy-in staff and entered directly in the system. Data collection is performed either using paper-based forms or mobile data collection using electronic forms. Data entry operators key in the data in the MEL MIS. Mobile data collection is entered directly in the system – in the case where there is a real-time internet connectivity to the MEL MIS; or collected in offline mode and uploaded in the system once connection is restored or available. In both cases, the data is verified by the system through business rules, lookup codes and syntax verification. Based on the data entered, the MEL MIS refreshes the indicator values based on the configured indicator formula for each indicator. Data reporting and analytics is performed using the MEL MIS reporting component or more elaborate data analytics tools such as Tableau, Power BI and Metabase.

The second scenario is where the Buy-in or the Implementing Partner (IP) use their own M&E system to capture, store, and track indicator data. Figure 2 below shows the data flow from the external M&E system to the MEL MIS. Data is collected and verified by the Buy-in/IP team. The Buy-in/IP batch upload their M&E data in the MEL MIS through a web-based client program. The upload process verifies the data applying the MEL MIS business rules prior to upload and storing the data in the system. Once the data is uploaded, the MEL MIS refreshes the indicators using the configured indicator formula for the indicators impacted by the uploaded data. All data entered in the system must be at a granularity level that meets the defined disaggregation requirements for each indicator. Similar to the previous scenario, the USAID CATALYZE HQ MEL team performs data reporting and analytics using the MEL MIS reporting component and dashboard or external data analytics tools such as

Tableau or Power BI.

Figure 2- Buy-in/Implementing Partner use external M&E



7. MEL MIS Requirements

The system requirements are divided into two major categories: Functional and Technical requirements. The functional requirements are further divided into six categories: general, beneficiary, indicator, activity, compliance, security and access Control, and dashboard, reporting and GIS. The technical requirements are divided into four categories: access control, security, compliance, and operations.

The requirements in this document are classified using the MoSCoW terminology detailed in the table below.

Table 2 - MoSCoW Requirements Terminology

Value	Rating	Description
1	Must (M)	Defines a requirement that has to be satisfied for the final solution to be acceptable.
2	Should (S)	High-priority requirement that SHOULD be included if possible, within the delivery time frame.
3	Could (C	Desirable or nice-to-have requirement (time and resources permitting) but the solution will still be accepted if the functionality is not included.
4	WON'T or WOULD (W)	Requirements that stakeholders want to have, but have agreed will not be implemented in the current version of the system.

7.1. Functional Requirements

Table 3 – Functional Requirements

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
General / Base Functionality				
FRG-001	1	Ability to create custom forms for data entry	Buy-ins capture activity data, beneficiary profile data – and use the forms to enter data in the system	Buy-Ins
FRG-002	2	Ability to define template forms to be used for Buy-ins to use	Allow for standard data entry forms and Excel templates	Buy-Ins
FRG-003	1	Ability to include details tabular sections in a form	Example activity form, with a tabular section for beneficiaries impacted by form	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRG-004	1	Offline capability for all forms	Buy-in use mobile data collection with no real-time access to the system	Buy-Ins
FRG-005	1	Ability to sync with the system once internet access is available/restored	Mobile data collection automatically synced with system once access is available	Buy-Ins
FRG-006	1	Batch processes for functions such as bulk upload and bulk modify	Buy-ins have the need to upload bulk data (e.g. 100 records at a time) in the system. For example paper based data collection, entered/verified in Excel and bulk uploaded in the system	Buy-Ins
FRG-007	1	Batch processes must continue to operate despite loss of connection between client and system	When a Buy-in starts a batch process, the batch process should not be interrupted when Buy-in loses power or connection to the system. Add / elaborate: A batch process is started by the end user through a system module/function through the browsers. The system executes the batch process on the server and communicates progress to the end user interface. When a connection is lost, the process should continue to execute on the server and updates the user in offline mode (following requirement)	Buy-Ins
FRG-008	1	Batch processes must log errors and output to log files and emailed to specified group of users	Allows Buy-in to track batch process results even when connection is lost	Buy-Ins
FRG-009	1	System messages must be informative and user friendly	System should provide information error and warning messages to allow user to easily rectify the problem	Buy-Ins
FRG-010	1	System must perform as much as feasible syntax checking	Minimize user / inaccurate data entered in the system	Buy-Ins
FRG-011	1	System must implement semantic business rules verification on data entered	Minimize user/inaccurate data entry in the system	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRG-012	1	Capability to define lookup tables for disaggregation criteria	Disaggregation criteria for example geographical hierarchy, gender, company type, beneficiary type.	Buy-Ins
FRG-013	1	Ability to flag data for public view	Vetted / approved data for public can be viewed / accessed for reporting by external entities	Buy-Ins
FRG-014	1	System should allow for the upload of quantitative and qualitative data including the upload of report documents	Buy-ins should have the ability to upload pdf, Word, image and other non-quantitative data files.	Buy-Ins
Functional Requirements - Beneficiary				
Beneficiary in this context denotes the standard use of the term such as the MSME, households, schools, and other enterprises; it also denotes the intermediary actors such as the credit unions, financial institutions, etc who are also part of the programs.				
FRB-001	1	Ability to define multiple Beneficiary Profiles. Each beneficiary profile shall have its own set of attributes. The system shall have the capability to define multiple beneficiary profiles. Beneficiary profiles can be individual beneficiaries – such as youth/person; household beneficiaries; entities – such as Financial Institutions, Schools, MSME partner beneficiaries – such as financial institutions end-user beneficiaries – households, youth, MSME, …	Buy-ins have different beneficiaries and profiles. For MS4G – MSMEs and Intermediary Financial Institutions are two types of beneficiaries; For EduFinance – beneficiaries are Schools participating in the program, Financial Institutions	Buy-Ins
FRB-002	1	Ability to modify a beneficiary profile.	Buy-ins may have to add new attributes to a beneficiary profile depending on the program requirement	Buy-Ins
FRB-003	1	Ability to create new beneficiary instances	New beneficiaries participating in the program	Buy-Ins
FRB-004	1	Ability to modify beneficiary instances	Beneficiary data may change such as geographic location	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRB-005	1	Capability to uniquely identify a beneficiary in the system within a beneficiary profile type	May have multiple beneficiaries with same name	Buy-Ins
FRB-006	1	Search for beneficiaries based on a set of attributes (with filters, etc)	Buy-ins have the need to look up beneficiary data	Buy-Ins
FRB-007	1	Free search for beneficiaries based on a keyword or a string	Buy-ins have the need to search for beneficiaries based on a keyword	Buy-Ins
FRB-008	1	Batch process – ability to upload beneficiary data in bulk	Buy-ins may have beneficiary data in Excel file to upload in system	Buy-Ins
FRB-009	1	Bulk update – ability to update one or more attributes of beneficiaries in bulk	Buy-ins have the need to bulk update beneficiary data in the system	Buy-Ins
FRB-010	1	Ability to permanently purge beneficiary data from the system	Buy-ins may have the need to purge a beneficiary profile for data privacy compliance	Buy-Ins
Functional Requirements - Indicator				
FRI-001	1	Ability to define Buy-in level indicators.	Each Buy-in has its own set of indicators	Buy-Ins
FRI-002	1	Ability to define program / USAID CATALYZE level indicators	USAID CATALYZE has a set of indicators that are global to all Buy-ins	USAID CATALYZE
FRI-003	1	Ability to define levels of disaggregation for each indicator	All Buy-ins have a set of disaggregation attributes	Buy-Ins
FRI-004	1	Indicator calculation – indicators can be calculated automatically, or user entered	Templates are not standard and need to be customised on a project-by-project basis	Buy-Ins
FRI-005	1	Automated indicator calculation – define formulae to automatically update indicator value based on data entered	Based on the indicator formula, indicator must be updated based on the data elements entered	Buy-Ins
FRI-006	1	Manual indicator – users must have the ability to enter indicator values manually	There may be some indicators that are not formula based	Buy-Ins
FRI-007	1	Indicator formula definition must be privileged function	Access to create indicator formulae must be limited to privileged users	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRI-008	1	Indicator formula/definition updates must be privileged function	Access to indicator formula modification must be limited	Buy-Ins
FRI-009	1	The system must allow for logical indicator deletion. This must be a privileged operation	During the life of the program, some indicators may be deactivated	Buy-Ins
FRI-010	1	Permanent indicator deletion must be a restricted operation (super user)	During the life of the program, some indicators may be no longer required	Buy-Ins
FRI-011	1	Ability to modify indicator definition, including frequency and formula	During the life of the program, an indicator definition may change	Buy-Ins
FRI-012	1	System must allow for elaborate/complex indicator calculation	An indicator may have a complex formula based on % of other indicators	Buy-Ins
FRI-013	1	Allow for indicator disaggregation based on some or all of the disaggregation criteria defined in Appendix B	Current disaggregation criteria is defined in Appendix B. Additional criteria may be defined	Buy-Ins
FRI-014	2	System must allow to define future disaggregation criteria	Additional disaggregation criteria and granular data may be collected to address new disaggregation requirement	Buy-Ins
FRI-015	1	Multiple tracking period – monthly, quarterly, semi annual, annual, etc.	Indicator reporting may vary depending on the activity or the Buy-in	Buy-Ins
FRI-016	1	Indicator format may be count, percentage, sum	Indicator can be number of women, percentage of schools or totals	Buy-Ins
FRI-017	1	Indicator tracking on target vs. actual and allow for adjustments	Feature allows senior managers to track program performance with goals	Buy-Ins
Functional Requirements - Activity				
FRA-001	1	Activities data – define attributes for each type of activity. Be able to define the same type of activity, but different attributes depending on the Buy-in and the activity. Activity types include: events, trainings, outreach, workshops.	Buy-ins have different activities, track attendance	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
		Activity attributes include date of activity, number of attendees, location, activity type, objective.		
FRA-002	1	Capability to define and modify attributes for the various activity types, including before/after photos and other qualitative information	Buy-ins may decide to track additional information for activities	Buy-Ins
FRA-003	1	Ability to flag fields as privileged within an activity	Required for responsible data and GDPR compliance	Buy-Ins
FRA-004	1	Ability to uniquely define activities for ease of lookup	Define an intuitive format for Activity and other Identifiers in the system for each of lookup	Buy-Ins
FRA-005	1	Ability to create data entry forms for the different activity types	Buy-in data entry MEL team uses system forms to enter data	Buy-Ins
FRA-006	1	Ability to track attendees – target vs actual for each activity and link attendees to beneficiaries in the system where applicable	Feature provides capability to analyse planned versus actual attendance	Buy-Ins
FRA-007	1	Enter new activity data using New Activity forms defined in FRA-005	Buy-in data entry	Buy-Ins
FRA-008	1	Ability to modify activity data	Privileged users should be able to edit activity data	Buy-Ins
FRA-009	1	Delete activity data	Privileged users should be able to delete entered activity data	Buy-Ins
FRA-010	1	Bulk upload activity data	Buy-ins may have activity data in Excel file to upload in system	Buy-Ins
Functional Requirements – Compliance, Security, and Access Control				
FRS-001	1	Create roles such as data entry, MEL lead, system admin, viewer, USAID CATALYZE MEL	Users' access to functions and features in the system based on their role	Buy-Ins
FRS-002	1	Specify access permissions to functions and features in the system based on the defined roles	Limiting functions and features based on role	Buy-Ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRS-003	1	Ability to specify access limit at field level and record type	For data privacy compliance, privileged users should have access to data flagged as private	Buy-Ins
FRS-004	1	Limit access to data based on value of a field in a record	External users can only view data records which are flagged for public consumption	Buy-Ins
FRS-005	2	Multi-factor authentication for system users	Increased security	Buy-Ins
FRS-006	1	Ability to permanently purge fields/records/personal identifiers linked to specific individuals who request deletion	Required for GDPR compliance	Buy-Ins
FRS-007	1	Encrypted identification fields for individual records	Record IDs (especially those containing personal identifying information) need to be secure.	Buy-Ins
Functional Requirements – Dashboard, Reporting, and GIS				
FRR- 001	1	Ability to generate consolidated reports at the global, regional, and cluster levels	Senior managers need to see consolidated and accurate reports that summarise key grant project metrics across a portfolio	Buy-Ins
FRR-002	1	Dashboard - users should have the capability to customize their dashboard based on their reporting and tracking needs, including charts, maps, and other data visualization and download these visualization to include in reports such as quarterly and annual reports	USAID CATALYZE and Buy-in users need to use dashboards to track at a glance performance of the program at the global USAID CATALYZE program or Buy-in level	Buy-Ins
FRR-003	1	Dashboard – GIS mapping and information should be visible in users' dashboards	Users should be able to view program performance pictorially on a map with the ability to zoom in on an area	Buy-ins
FRR-004	1	Dashboard – ability to drill down on summary / aggregate data in a dashboard	Managers need to view the details of aggregate summary data	Buy-ins
FRR-005	1	Report – system should have a set of pre-defined reports	These are standard data and indicator reports used across all Buy-ins and USAID CATALYZE program level	Buy-ins

Requirement #	Priority	Description	Rationale	Impacted Stakeholders
FRR-006	1	Report – ability to create branded report formatted templates	This is required to ensure management is generating reports that are USAID CATALYZE branded and compliant	Buy-ins
FRR-007	1	Ability to generate reports and share them externally with other users	USAID CATALYZE managers should be able to generate reports and share them through a link or as an exported document without loss of formatting	Buy-ins
FRR-008	1	Reports should adhere to the security / access level of users viewing report and when displaying the data	Same report can be viewed by different users; users should only be able to see the data accessible within their role privilege	Buy-ins
FRR-009	1	Ability to create custom and ad-hoc reporting without the need to contact the vendor	Program managers have the need to create one-off reports	Buy-ins
FRR-010	1	Ability to generate summary and disaggregate reports with drill down and analysis features	Program managers need to perform analysis on the data collected	Buy-ins
FRR-011	1	Ability for external users to search and view reports of vetted data and documents (content vetted and flagged for public use)	Allow USAID and external users access to vetted content	Reporting & Viewers
FRR-012	1	Searchable public report repository accessible to external public users login requirement	Allow USAID and external users to search for published reports	Reporting & Viewers

7.2. Non-Functional (Technical) Requirements

Include technical and operational requirements that are not specific to a function. This typically includes requirements such as processing time, concurrent users, availability, security, compliance.

Table 4 – Non-Functional Requirements

ID	Requirement
NFR-001	Access control: ability to create multiple user roles in the system.
NFR-002	Access control: ability to define, control, and govern access to system functionality, data – including limiting access based on value of specific field in a record, within the system based on user assigned role.

ID	Requirement
NFR-003	Access Control: Shared accounts to be actively prevented in favour of named user accounts.
NFR-003	Access Control: Palladium is able to easily review and independently manage its users' access privileges.
NFR-004	Access Control: Service provider has a formal identity and access management process to manage its access rights, the access rights are regularly (at least twice a year) reviewed.
NFR-005	Access Control: The system must not allow any person to carry out any action in the system unless the person is an authorised user who is successfully identified and authenticated.
NFR-006	Access Control: The system must allow an administrative role to set up and maintain users and user groups.
NFR-007	Access Control: The system must allow a user to be a member of one or more groups.
NFR-008	Access Control: The system must allow administrative roles to add and remove users to and from user groups at any time.
NFR-009	Access Control: The modification of users and user groups must be restricted to administrative roles.
NFR-010	Access Control: The system should allow carrying out of bulk operations on users and user groups.
NFR-011	Access Control: The system should allow admin users to see which user group(s) another user is a member of.
NFR-012	Access Control: The system must allow the changing of access settings by authorised users, at any moment (not only at the moment of creation).
NFR-013	Accessibility: The system supports SSO (single sign-on) with Azure explicitly referenced as a supported SAML identity provider. SSO should extend to deep links.
NFR-014	Accessibility: must be able to access the system through mobile devices without loss of functionality or features. The system must be able to operate across the globe in developed and developing environments where connectivity and coverage issues may be present.
NFR-015	Audit Logging: Audit logs can be integrated with Palladium's Security Information and Event Management (SIEM) solution: a standard log format must be used (e.g., syslog)
NFR-016	Audit Logging: The system allows administrators to produce records of user activity to support monitoring, incident response and investigations, including system administrators' activities. The granularity of the audit policy/settings that can be configured in the system should be provided.
NFR-017	Audit Logging: The audit logs are protected against unauthorized modification, deletion and access
NFR-018	Audit Logging: The system keeps an unalterable audit trail capable of automatically capturing and storing information about: • any action taken on any document (or version of a document), record or folder, any electronic workflow, or the classification scheme; • the user undertaking the action; • the date and time of the action.

ID	Requirement
NFR-019	Audit Logging: The system allows sorting of the audit trail per type of action, and listing per descending date
NFR-020	Audit Logging: The audit logs can be retained for a customer-configurable period.
NFR-021	Business Intelligence: It is possible to connect to the database or reporting services using a Business Intelligence tool (eg. Microsoft Power BI).
NFR-022	Compliance: must allow branding of the look and feel of the solution.
NFR-023	Compliance: data must be safeguarded in the system under the guidelines of GDPR and USAID Responsible Data requirements.
NFR-024	Compliance: system must comply with the privacy guidelines stated in USAID ADS 508.
NFR-025	Compliance: system must meet the IT system guidelines stated in USAID ADS 509.
NFR-026	Compliance: long-term storage and Palladium ownership of all information stored on the system. Information should be retained on the system for several years (variable based on client) past the closing of a project. All information stored on the system should be owned by and accessible to Palladium.
NFR-027	Compliance: system must adhere to open technology standards and not be a closed proprietary technology.
NFR-028	Compliance: The solution is compatible with the current versions of MS Edge, Firefox, Google Chrome and Safari. The system is expected to support all future versions of these browsers.
NFR-029	Compliance: Comprehensive backup regimes are implemented to ensure compliance with regulatory, statutory, contractual and business requirements.
NFR-030	Configuration: It is possible to configure modules. e.g. page layouts, custom fields, picklist values, validation rules, workflows, etc.
NFR-031	Configuration: The look and feel of the solution can be configured to Palladium specifics, e.g. branding, logo, fonts, etc.
NFR-032	Configuration: The look and feel of the reports can be configured to Palladium specifics.
NFR-033	Configuration: Custom report creation and editing providing functionality such as the addition and removal of fields, grouping, sorting, filtering, etc.
NFR-034	Configuration: The solution supports the ability to record monetary amounts in different currencies whilst maintaining a system functional currency for reporting and other global purposes.
NFR-035	Configuration: The solution supports mechanisms to record and update exchange rates for the defined currencies at user configurable periods.
NFR-036	Customization: It is possible to customise the modules.
NFR-037	Customization: Any customisation of the system must be performed minimising the impact on upgradeability of the system to future releases, to ensure that the system can be easily upgraded to future product releases maintaining Palladium-specific customisations.

ID	Requirement
NFR-038	Customization: The supplier is requested to describe the customisation approach proposed for this purpose.
NFR-039	Customization: Any customisation performed by the supplier must be provided to Palladium in a form that enables Palladium to use it, maintain it and modify it independently of the supplier.
NFR-040	Data Protection: The Data Security Architecture has been designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)
NFR-041	Data Protection: All forms containing sensitive information have disabled client-side caching, including auto complete features
NFR-042	Data Protection: For web-based applications, all sensitive data must be sent to the server in the HTTP message body (i.e. URL parameters are never used to send sensitive data)
NFR-043	Data Protection: Personal data can be stored only temporarily on the web front server.
NFR-044	Data Protection: Personal data (e.g., submitted through forms, kept in logs, etc) can be removed from the system at the end of its retention periods, which can be administratively defined. This can be performed by an administrator.
NFR-045	Data Protection: Documentation exists that establishes and defines your encryption management policies, procedures, and guidelines
NFR-046	Data Protection: Capabilities exist to allow the creation of unique encryption keys per customer.
NFR-047	Data Protection: List any third party/open source/proprietary frameworks used to manage encryption keys.
NFR-048	Data Protection: The solution has a feasible option to encrypt all data, e.g., by using application, database or disk level encryption. The encryption mechanism and key management should be described.
NFR-049	Data Protection: All data stored in backups is in encrypted format.
NFR-050	Data Protection: Any media (also broken disks) used to store personal data must be wiped, degaussed or physically destroyed when disposed of or before handed over to a 3rd party.
NFR-051	Data Protection: All files uploaded to the system must be virus scanned on a dedicated system before stored or processed.
NFR-052	External Systems: The system supports and provides required methods for integration with mature web services platforms.
NFR-053	External Systems: Create, Read, Update and Delete operations are exposed via web services to all data sets within the system.
NFR-054	External Systems: Web Services documentation is available upon request.
NFR-055	External Systems: The system supports triggers to provide real time integration with external dependent systems.

ID	Requirement
NFR-056	General: The system supports bulk Excel/Csv import and export.
NFR-057	General: Share Service Level Agreement, SLA, for end user support including actual achievements for the last 12 months.
NFR-058	Governance and Risk Management: Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?
NFR-059	Governance and Risk Management: Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?
NFR-060	Governance and Risk Management: Do you conduct risk assessments associated with data governance requirements at least once a year?
NFR-061	Governance and Risk Management: Do you provide customers with documentation describing your Information Security Management Program (ISMP)?
NFR-062	Governance and Risk Management: Do you have agreements to ensure your providers adhere to your information security and privacy policies?
NFR-063	Governance and Risk Management: Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? Please list.
NFR-064	Governance and Risk Management: Are systems compliant with GDPR and other information protection regulations.
NFR-065	Human Resources: Do you specifically train your employees regarding their specific role and the information security controls they must fulfil?
NFR-066	Human Resources: Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?
NFR-067	Human Resources: Are personnel trained and provided with awareness programs at least once a year?
NFR-068	I/O Data Validation, Session Management, Error Handling: The system is designed and configured to validate all data input to ensure that it is safe for use within the system. The system input validation checks implemented should be described in detail.
NFR-069	I/O Data Validation, Session Management, Error Handling: The system should be designed and configured to validate all output data to ensure that internal processing is being performed correctly and that the data is safe for external applications.
NFR-070	I/O Data Validation, Session Management, Error Handling: The system uses and manages sessions in a secure manner. All session management implementation and settings should be described in detail.
NFR-071	I/O Data Validation, Session Management, Error Handling: The system must be configured to prevent the output of sensitive information in error messages.

ID	Requirement
NFR-072	Maintenance: The system provides bulk data management, including bulk upload and meta-data changes tools, to facilitate technical system maintenance. Bulk updates should also be possible to comply with retention policies, in a controlled manner (jobs should be easy to schedule and monitor for this).
NFR-073	Maintenance: The system provides functionality to support archiving and purging tasks, configurable based on meta-data parameters; archiving and purging tasks can be executed as scheduled jobs.
NFR-074	Maintenance: The system allows to define a set retention policy based on a set of parameters, to be run either online or as scheduled jobs.
NFR-075	Maintenance: All data management tasks can be performed by Palladium independently (no support/service ticket required)
NFR-076	Operation: system must operate in offline mode and automatically sync when internet connectivity is restored.
NFR-077	Operation: system must be hosted in a secure environment with access to the backend and data repository restricted to authorized staff only.
NFR-078	Operation: backup and Disaster Recovery strategy for Business Continuity Plan.
NFR-079	Operation: high system response time, for daily data functions (entry, changes, saving, etc) and reporting. The system must have adequate stability to handle period of high access demands such as end of periodic batch data upload and reporting
NFR-080	Operation: system must be extensible, functional and performance, to be able to meet future performance needs and additional functionality. Ability to extend the functionality of the system through API programming per needed base and timeline.
NFR-081	Operation: system must have APIs and backend capability to integrate with other systems. Integration can be bi-directional, where data is retrieved from the system or data is uploaded in the system.
NFR-082	Operation: vendor must be able to provide 24*7*365/6 support. SLAs: Robust SLAs ensuring a high level of system performance backed by Service Credits.
NFR-083	Operation: system must support multi-lingual data stored in the data repository; front end user interface; and user error and other system messages.
NFR-084	Operation: system must be able to operate adequately in challenging environments where power and internet connectivity are intermittent. System must be light on graphics, visually lean with greater emphasis on functionality and features.
NFR-085	Operation: ability to upload data in batch format with offline completion log and error reporting.
NFR-086	Operation: ability to integrate with other systems/tools such as PowerBI or other analytics and reporting tools.
NFR-097	Operation: system can be licensed as SaaS (Software as a Service) or on-premise installation if required.
NFR-089	Operation: The solution is implemented as an integrated system, preferably with a centralised repository where all data and metadata is stored and provides one frontend that allows full control of the data.

ID	Requirement
NFR-090	Operation: The system can cope with at least 100 concurrent users
NFR-091	Operation: The system can cope with unlimited number of records and associated records
NFR-092	Operation: The system can cope with an unlimited number of linked or attached documents or content
NFR-093	Operation: Android and iPhone Apps that compliments browser functionality. Alternatively a modern responsive UX is used that renders the system effectively on different devices.
NFR-094	Operation: Logically and physically separated development, test and production environments are available with required refresh and publishing mechanisms provided to support development practices.
NFR-095	Operation: The solution is accessed directly from the Internet without the need of VPN or similar technology.
NFR-096	Operation: Mean time to repair and mean time to restore are in alignment with industry best practices and referenced in contractual material.
NFR-097	Operation: Business continuity plans are subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness. A test summary will be shared with Palladium upon request.
NFR-099	Performance: The solution should provide a dynamic and responsive web frontend using the latest technologies and standards, based on the browser specification provided. The supplier should describe the different logical components used by the solution to support this web frontend, and detail any addon or plugin used (if any), as well as the libraries used (e.g. JavaScript etc).
NFR-100	Performance: The supplier shall include dedicated performance and capacity validation tests as part of each release. A description of how this is approached by the supplier for major and minor releases should be provided.
NFR-101	Performance: Maximum upload/download internet bandwidth of 100kbps and 300 kbps respectively per user session.
NFR-102	Performance: Support network latency of 400ms.
NFR-103	Performance: What technologies are used to enhance the timeliness of the user experience?
NFR-104	Secure Software Development: The vendor implements a software security lifecycle process to actively identify security risks and requirements for the solution. The solution has been developed using secure coding good practices (e.g., from Microsoft SDL or OWASP Development Guide). The solution has been tested for security vulnerabilities throughout the development lifecycle, e.g., against guidance such as the OWASP Top Ten Risks or the SANS Top 25 programming errors.
NFR-105	Secure Software Development: The vendor implements a vulnerability management process to actively identify and remediate technical vulnerabilities, and disseminates information, patches, and remediation guidance for technical vulnerabilities in a timely manner to customers.
NFR-106	Secure Software Development: Documentation is available upon request that describes the quality assurance processes.

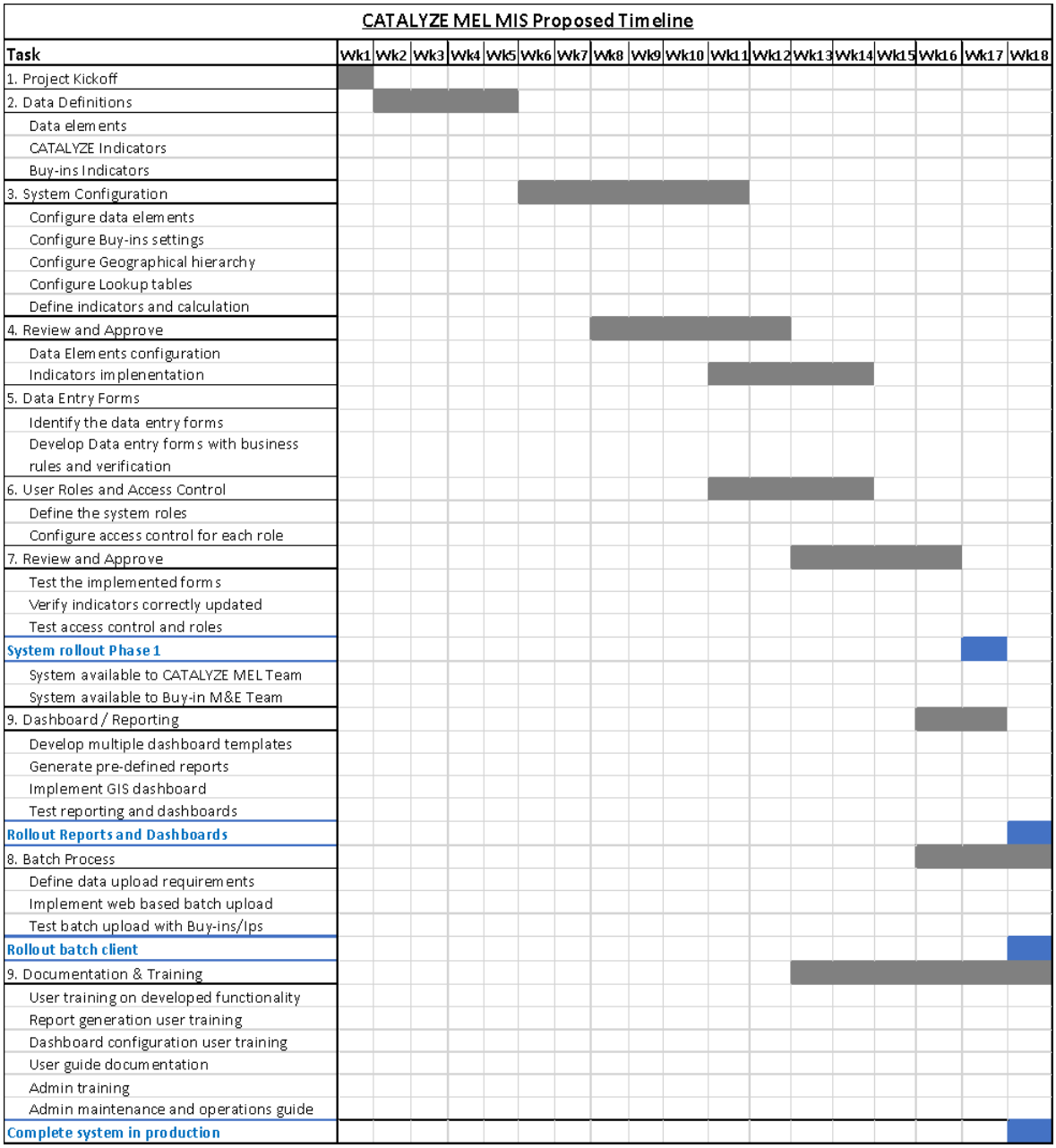
ID	Requirement
NFR-107	Security: system should authenticate users prior to granting access to the system. MFA and SSO options are desirable.
NFR-108	Security: system limits number of incorrect authentications with access denied option.
NFR-109	Security and Compliance: ability to encrypt specific data elements if necessary and permanently purge data elements.
NFR-110	Security: web-based functions/interfaces must be accessed using HTTPS secure protocol. Batch non web-based processes should authenticate through a secure connection.
NFR-111	Security: hosting should be on a USAID approved hosting security requirements and location.
NFR-112	Security: The solution can be configured to suspend and shut down inactive sessions after a predefined period of time.
NFR-113	Security: The solution should provide mechanisms to manage the risks posed by all forms of malicious code. The mechanisms used to protect against malicious code should be listed.
NFR-114	Security: The hosting service provider regularly (at least annually) assess security risks of the service. The summary of risk assessment is reported to Palladium.
NFR-115	Security: You ensure that security threat detection systems using signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted time frames.
NFR-116	Security: Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) are implemented.
NFR-117	Security: Ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises are monitored, controlled and isolated from data storage and process.
NFR-118	Security: Secure socket layer (SSL) protocol is used for all HTTP connections. Only valid SSL certificates signed by commonly trusted CA can be used (e.g. self-signed certificates cannot be used). TLS 1.2 or higher used.
NFR-119	Security: System and network environments are protected by a firewall or virtual firewall to ensure business and customer security requirements.
NFR-121	Security: Technical measures and defence-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks are applied
NFR-122	Security: Physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) is anticipated and designed with countermeasures applied.

ID	Requirement
NFR-123	Security: Data centers are NOT located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.).
NFR-124	Security: A 3rd party performs regular security / penetration test to the system. Results are shared with Palladium upon request.
NFR-125	Security: Systems are in place to monitor for privacy breaches and you notify customers expeditiously if a privacy event may have impacted their data.
NFR-126	Service Level Agreement: Financially backed service level agreements defining system availability.
NFR-127	Service Level Agreement: List scheduled maintenance or outage windows.
NFR-128	Service Level Agreement: Share Service Level Agreement, SLA, for end user support including actual achievements for the last 12 months.

8. Proposed Timeline

The proposed timeline is focused on the implementation of the MEL MIS. The timeline does not include the procurement period, but instead has a start date after the completion of the solution and implementing vendor selection. The proposed timeline identifies the main tasks and milestones for the implementation of the system without enforcing any project implementation methodology; although it is strongly recommended that the system is implemented using the Agile methodology with two-week sprints to ensure the system is implemented correctly based on required specification.

Figure 3- Proposed USAID CATALYZE MEL MIS Implementation



9. Appendices

1. Appendix A: USAID CATALYZE Buy-ins

The table below provides a list of USAID CATALYZE identified Buy-ins along with the countries they operate in and the sectors they are engaged in. These Buy-ins were selected for interviews because they are representative of the different Buy-in types within USAID CATALYZE; some Buy-ins are implementing in multiple countries, working with multiple implementing partners, and have their own MEL systems, while others are implementing in a single country and have a local Palladium team in charge of implementation including dedicated MEL staff. Interviewing these different Buy-in types allowed us to gather a comprehensive list of requirements that capture the various needs across user types and data flows.

The information in this table is based on the status of USAID CATALYZE as of the date of this report. More Buy-ins or additional countries and sectors may be added/removed to/from the program.

Table 5- List of Buy-ins that have completed their MEL plans

#	Buy-in	Description	Country(ies)	Sector(s)	Approved MEL Plan
1	USAID Edfinance	The 5-year USAID USAID CATALYZE EduFinance program seeks to improve and sustain learning outcomes of disadvantaged children and youth.	Democratic Republic of Congo, Zambia, South Africa *More to be added*	Education	Yes
2	USAID Ethiopia — Market Systems for Growth	MS4G is focused on enhancing market systems in Ethiopia to facilitate business growth, create employment, and promote the development of the foundational elements for continued, transformational, and inclusive growth.	Ethiopia	Economic Growth	Yes
3	USAID Sahel — Finance for Resilience	The purpose of the USAID USAID CATALYZE Sahel Finance for Resilience activity is to improve the access and flow of finance and investment to agriculture stakeholders and youth entrepreneurs in Burkina Faso and Niger.	Burkina Faso, Niger	Agriculture, Economic Growth	Yes
4	USAID Western Balkans — Engine of Growth	The purpose of the EoG Activity is to facilitate Western Balkan SME growth and productivity by improving their access to and utilization of finance.	TBD	Economic Growth	Yes

2. Appendix B: Interviews

Table 6- List of interviews conducted to gather requirements for the MEL MIS

#	Buy-in	Interviewee(s)	Date of interview	Role
1	USAID CATALYZE-wide	[redacted]	3/4/21	Senior MEL Manager
2	MS4G		3/22/21	MEL In-Country Lead
3	Palladium's GMS[1] (not a USAID CATALYZE Buy-in)		3/18/21 & 3/31/21	Lead on GMS development
4	EduFinance		3/26/21	-Sr. MEL Advisor -Education Specialist/MEL
5	EoG		4/5/21	Manager
6	F4R		4/5/21	-Director, Economic Growth -Project Manager
7	EduFinance		4/16/21	Implementing Partner
8	USAID CATALYZE Project Management (not a USAID CATALYZE Buy-in)		4/29	Project Manager
9	Palladium IT team (not a USAID CATALYZE Buy-in)		5/12/21	Palladium's IT Management Team

[1] GMS = Grants Management System

3. Appendix C: Disaggregation Criteria

There are several disaggregate criteria defined at USAID CATALYZE program level and Buy-in level. Some disaggregation criteria are common to all Buy-ins and others are specific to a Buy-in. This appendix provides a sample of the disaggregation criteria defined for the USAID CATALYZE program.

Geography – for each country, collected data is associated with the official administrative geographic location of the country the Buy-in operates in. Additionally, data may be attributed to the region of a Buy-in's country of operation.

Gender – defined by USAID CATALYZE and will be used across all Buy-ins.

Sector – each USAID CATALYZE Buy-in has a set of sectors defined such as Education and Economic development. USAID CATALYZE shall provide a list of all the sectors and sub-sectors, where applicable.

Age – beneficiaries participating in the program are categorized by age groups. The Age group definitions shall be the same across all Buy-ins. USAID CATALYZE shall provide the list of the Age groups.

Disable/Not Disabled – some Buy-ins may track beneficiaries with disabilities.

Activity Type – Buy-ins track their activities by activity type. There may be common activity types across all Buy-ins and ones specific to a Buy-in.

Actor categories – entities such as financial institutions, schools, banks, and farms are categorized by a business type and subtype. Some MSME types may be the same across all Buy-ins and others are specific to a Buy-in. Examples include schools such as Primary, Secondary, Vocational; School type Faith based, non-profit, private, public; Financial Institution such as Bank, Credit Union, Microfinance.

Business line – define the business focus of the entity participating in a program. For example the list of crops for a farm.