Pondera

Glossary of Terms

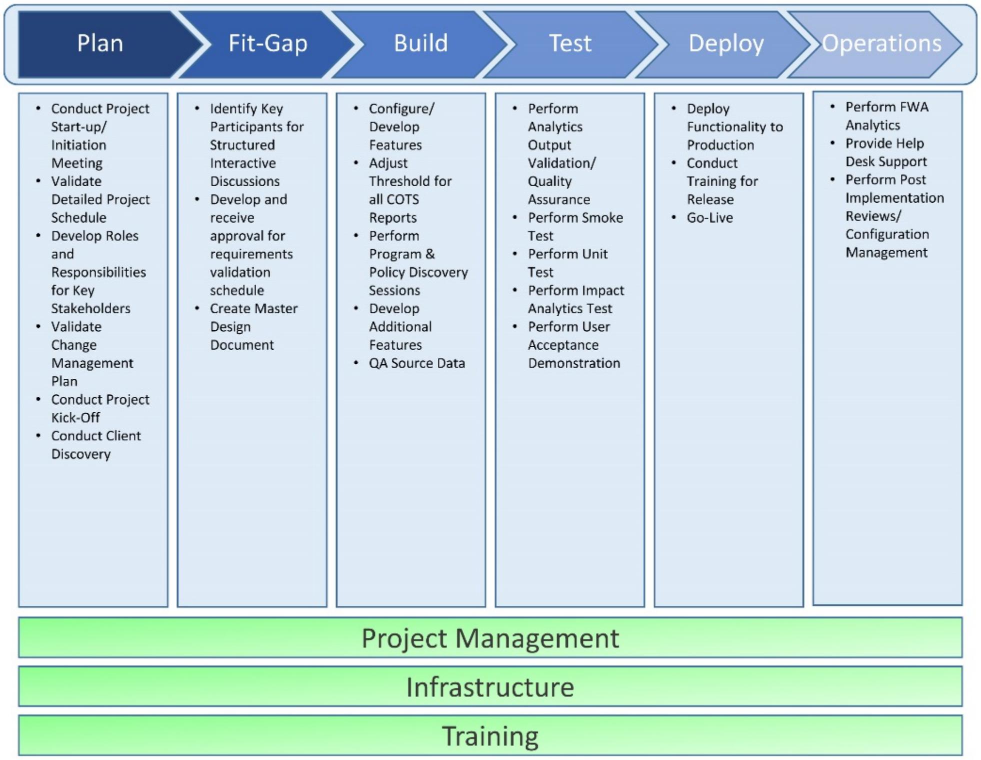
Project Management Terms

Master Design Document (MDD) – The MDD is an excel workbook with multiple tabs demonstrating all of the elements for each application or section planned for the FDaaS dashboard. The workbook includes a worksheet for each dashboard "tab" and core feature in the FDaaS dashboard including all of the following:

- Super Search
- Main Tab (including reports and their associated logic descriptions, filters, matrix grids)
- Retailer and Recipient Profiles (including indicators, maps/street view)
- Geospatial Maps
- Other "tabs" including Account, Special Investigations

Project Requirements and Onboarding Process (PROP) – The PROP is a proven, interactive fit-gap process designed specifically for FDaaS implementations. During the PROP, we will validate requirements, complete a security plan, gather information for threshold and model tuning, identify and evaluate source data files, and perform other implementation-specific functions.

Pondera brings technical, statistical and investigative resources to PROP sessions. The Steps in the PROP are: Planning; Fit-Gap; Build; Test; Deploy; and Operations.



Plan	Fit-Gap	Build	Test	Deploy	Operations
• Conduct Project Start-up/ Initiation Meeting • Validate Detailed Project Schedule • Develop Roles and Responsibilities for Key Stakeholders • Validate Change Management Plan • Conduct Project Kick-Off • Conduct Client Discovery	• Identify Key Participants for Structured Interactive Discussions • Develop and receive approval for requirements validation schedule • Create Master Design Document	• Configure/ Develop Features • Adjust Threshold for all COTS Reports • Perform Program & Policy Discovery Sessions • Develop Additional Features • QA Source Data	• Perform Analytics Output Validation/ Quality Assurance • Perform Smoke Test • Perform Unit Test • Perform Impact Analytics Test • Perform User Acceptance Demonstration	• Deploy Functionality to Production • Conduct Training for Release • Go-Live	• Perform FWA Analytics • Provide Help Desk Support • Perform Post Implementation Reviews/ Configuration Management

Project Management

Infrastructure

Training

System Security Plan (SSP) – The purpose of the SSP is to provide an overview of the security requirements of the system and describe the controls in place or planned, responsibilities, expected behavior of all individuals who access the system and identifies what specific data will be used and matched against third party sources.

Third Party Data Sources – To deliver the requirements for FDaaS, Pondera acquires and integrates data from several third party data companies. As part of the system security plan, Pondera articulates what specific data fields will be required from the state's systems and how that data will be matched against third party sources.

Timeline Dependencies – For FDaaS and Case Management projects, Security and Data Layout Specifications and have to be executed and approved in order for Pondera to receive any data.

FDaaS Dashboard Terms

Alert Subscriptions – These are located on the main tab, lists all of the available alerts.

Alert Details – The actual results of the analytics.

Alert Results – Flags shown in the alert results frame are the product of Pondera's analytics.

Apps Tab – Short for Applications. This tab provides the user with direct access to databases and advanced tools to further support their investigative efforts.

Beneficiary / Recipient / Claimant Tab – The tab located within the dashboard that allows an investigator to search for information regarding a specific beneficiary within the database.

Batch – The batch number represents the data group that contained information causing the flag to trip. Can be sorted from oldest to most recent and vice versa by clicking "batch."

Batch Range – The tool under the export tab that allows the user to choose the range of batches that they want to view for a particular flag.

Claims Detail Button – This button allows the user to view 10 claims either directly related to the cause of the flag, or the 10 most recent claims.

Export Tab – This tab provides the user with the ability to export selected flag IDs or batch ranges to Microsoft Excel.

FDaaS – Fraud Detection as a Service (FDaaS) is Pondera's advanced fraud, waste, and abuse detection and prevention solution. Our integrated system spans fraud detection, investigation and enforcement.

Flag – The numeric designation for each alert that may be moused over to view the flag name or clicked to access the flag details.

Flag Action – Reflects actions by the user, or other system users, relating to a specific flag.

Flag Watchlist – Serves as a condensed list of suspect flags populated by the user for further review. Flags are added to the watchlist by clicking the green watchlist button located in the Alert Details section of any flag.

Flag Name – The brief description that explains what the flag represents.

Flag ID – The numeric designation for each flag that may be moused over to view the flag name or clicked to access the flag details.

Fusion Table – Tables and/or charts uploaded to the FDaaS system to build link analysis templates to explore relationships among program participants.

Geospatial Tab – The tab that allows the user to load interactive maps in order to view either beneficiaries or retailers and be able to view commonalities between the two.

Link Analysis – Link is an analysis tool within FDaaS that allows users to visually display connections or relationships between organizations or individuals.

LTD – Life to Date.

Map Functions – Includes a drop down menu where users can load different maps to view.

Map Display – The window that presents the results for the selected map.

Matrix Grid – Visually provides a global look at program data under a variety of criteria. The grids are color coded to indicate potential areas of concern based upon Matrix Grid type as well as grid criteria.

PII – Personally Identifiable Information.

Rank – If applicable, the rank demonstrates the severity of the breach for a particular alert definition. Rank 1's are most severe and rank 10's are the least severe.

Retailer / Provider / Employer Tab – The tab that allows the user to search for information regarding a specific retailer/provider / employer within the database.

Risk Score – The proprietary weighting and ranking system built and tuned by Pondera's investigative and statistical staff. It is continually updated based on additional data runs and the results of investigations.

Scorecard – Provides users with ready access to entities currently monitored on the scorecard and their associated Pondera Risk Score. The Scorecard allows users to rank their entire set of providers based on any combination of flags in the FDaaS system and also allows users to maintain custom ranking systems and compare the results of more than one system against their providers, to determine which appear on both lists.

Subject – The column that represents the entity or individual who is the subject or target of the specific alert.

Subject ID – The unique identifier associated with the subject of the flag.

Special Investigations Tab – The tab that allows the user to view data pertaining to a specific investigation on an interactive geospatial map.

Tier – FDaaS has five alert tiers characterized by a determination as to the level of severity and propensity for fraud. Ranks range from 1-5, with 1 considered as the most severe and 5 being the least severe.

Type – Each flag type is classified according to the central focus of the detection algorithm.

What's New Tab – The tab that provides users with ready access to both current and prior development efforts related to their programs FDaaS dashboard. Sections include: Current Version Information; Coming Soon; In Progress; Enhancements; and Release History.

Case Management Terms

Active Mode – A case or child document that is in a state where it is non-editable.

Admin – This tab in the settings portion of the Case Management system is reserved for the administrative functions. These include the 'cancelled cases' section, the 'holiday calendar' section and the 'standard responses' section.

Capture – The form to be filled out when creating a new case from within Case Management.

Case/Record Lock – When a second user opens a Case or Issue Record that is currently opened by another user, the case record will show a warning message at the top that states 'this case is locked by (user name). This means that the second user to open the case can view the case but will not be able to make any modifications. This prevents changes from being lost while the first user edits.

Child Document – A form (screen) or document that is added to a case. Child documents generally carry a many to one relationship with the case in that you can add multiple child documents to a given case. For example, Party, To-Do's, Files are all considered "Child Documents."

Document Library- This section of the Admin tab is reserved for uploading documents for your users to reference when using the Case Management application.

Edit Mode – A case or child document that is in a state where it is editable.

Files – This section contains a list of Files uploaded to the system of any kind. Users are able to filter this view by File type.

Forms – A child document section that contains a list of Forms of any kind. Users are able to filter this view by Form type. For example, Hearings, Trafficking, Investigation Summary etc.

History – This section acts as an audit trail for the user to view the actions performed on a case. To access the history of a particular case, click on the "history" tab in the cases view.

Notes – This section can be used as a good way to track any additional details that are not already tracked in the system. It can also be a good way of recording work that you have done with case that does not necessarily get recorded otherwise.

Parties – This section contains a list of Parties uploaded to the system of any type. Parties can be attached to cases and sorted/filtered by party name.

Picklists –A type of field found on the case and child documents, where the user has the ability to choose one option from a drop down menu.

Settings – This portion of the user manual explains the settings options of the Case Management System. Through this section, you will be able to configure workflows, escalations, notifications, set up users and more.

Status:

(New) – A case has no assigned owner.
(Open) – Case ownership has been assigned to an owner.
(Closed) – The case has been processed, resolution has been obtained, and the close button has been used.
(Cancelled) – A case that has been opened in error can be Cancelled so not to impact reports.

To-Do's – A child document within Case Management used to assign tasks to yourself or other users. Users are able to filter this view by To-Do type.

Users – Through this section, you will be able to set up users, activate/deactivate users, and change their details (including their user roles).

Workflow – This tab in the settings portion of your application will contain options to determine the system reactions to actions performed in the system.

Yellowfin – The advanced reporting tool that allows the user to create customized reports.