FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES

DATA GOVERNANCE AND STRATEGY DELIVERABLE #4

RESULTS ORIENTED ACCOUNTABILITY PROGRAM AND DATA ANALYTICS PROJECT

Date: 06/24/2016
Version: 2.00
# Table of Contents

## Section 1  Introduction and Executive Summary ......................................................... 5
  1.1 Background and Objectives ...................................................................................... 5
  1.2 Connection to the Results-Oriented Accountability Program .................................... 6
  1.3 Summary of Recommendations .............................................................................. 7
    1.3.1 Data Governance ............................................................................................... 8
    1.3.2 Data Management and Master Data Management ....................................... 8
    1.3.3 Data Sharing and Data Acquisition ............................................................... 9
  1.4 Overarching View .................................................................................................. 10
    1.4.1 Core Components – Data Acquisition and Management ............................ 13
    1.4.2 Core Components – Data Exploration ......................................................... 14
    1.4.3 Overarching Management Areas ................................................................ 14
    1.4.4 Information Management Delivery Model ............................................... 16
  1.5 Scope of This Document ....................................................................................... 17

## Section 2  Current State in Florida ............................................................................. 18
  2.1 Results from Interviews/Meetings ......................................................................... 18
  2.2 Results from Reviewing Existing Documentation .................................................. 19
  2.3 Existing Legislative and Regulatory Environment .................................................. 20
  2.4 Existing Data Sharing Agreements and Supporting Processes ............................. 21

## Section 3  Lessons Learned ...................................................................................... 23

## Section 4  Models Used by Other States and at the Federal Level .......................... 25
  4.1 Colorado .............................................................................................................. 25
    4.1.1 Data Governance ............................................................................................ 26
    4.1.2 Master Data Management .............................................................................. 29
    4.1.3 Data Sharing .................................................................................................. 30
  4.2 Kentucky ............................................................................................................. 31
    4.2.1 Data Governance ............................................................................................ 31
    4.2.2 Master Data Management .............................................................................. 32
    4.2.3 Data Sharing .................................................................................................. 33
  4.3 Tennessee ............................................................................................................. 33
    4.3.1 Data Governance ............................................................................................ 33
    4.3.2 Master Data Management .............................................................................. 34
    4.3.3 Data Sharing .................................................................................................. 34
  4.4 Virginia ................................................................................................................. 34
4.4.1 Data Governance ................................................................................................ 34
4.4.2 Master Data Management ................................................................................... 35
4.4.3 Data Sharing ....................................................................................................... 35
SECTION 5 RECOMMENDED STATE ............................................................................... 37
5.1 Data Governance ..................................................................................................... 37
  5.1.1 Functional Organization and Governance ........................................................... 37
  5.1.2 Data Governance Execution Model ..................................................................... 37
  5.1.3 Recommended Steps to Implement Data Governance ....................................... 39
5.2 Master Data Management .......................................................................................... 40
  5.2.1 Recommended Steps to Implement MDM .......................................................... 42
5.3 Data Sharing and Data Acquisition .......................................................................... 44
  5.3.1 Recommended Steps to Implement Data Sharing and Data Acquisition ............ 44
SECTION 6 FUTURE STATE IN FLORIDA ........................................................................ 46
6.1 Functional Organization and Governance Required to Support Future State ............ 46
  6.1.1 Goals and Objectives ...................................................................................... 46
  6.1.2 Organizational Hierarchy ............................................................................... 47
6.2 Data Sharing Agreements and Data Acquisition ........................................................ 48
SECTION 7 GAPS ............................................................................................................... 50
7.1 Data Governance and Data Management ................................................................. 50
7.2 Master Data Management ........................................................................................ 50
7.3 Data Sharing Agreements and Data Acquisition ....................................................... 51
SECTION 8 IMPLEMENTATION ROADMAP ..................................................................... 52
8.1 Overview ..................................................................................................................... 52
8.2 The Business Case for Change .................................................................................. 52
8.3 Initiatives, Timelines, and Tasks ................................................................................. 52
  8.3.1 Data Governance Initiative ............................................................................ 53
  8.3.2 Data Governance Timeline ............................................................................ 53
  8.3.3 Data Governance Task Descriptions ............................................................... 55
  8.3.4 Master Data Management Initiative ................................................................. 59
  8.3.5 Master Data Management Timeline ................................................................. 59
  8.3.6 Master Data Management Task Descriptions ................................................. 61
  8.3.7 Data Sharing and Data Acquisition Initiative ................................................. 65
  8.3.8 Data Sharing and Data Acquisition Timeline ............................................... 65
  8.3.9 Data Sharing and Data Acquisition Task Descriptions .................................. 67
SECTION 9 CONCLUSION ................................................................................................. 71
SECTION 10  APPENDICES ..............................................

10.1 Appendix 1 – Meeting Notes From Current State Meetings................................. 72
   10.1.1 First Meeting ........................................................................................................ 72
   10.1.2 Second Meeting ................................................................................................. 72
   10.1.3 Third Meeting .................................................................................................... 73
   10.1.4 Fourth Meeting ................................................................................................. 73
   10.1.5 Fifth Meeting ..................................................................................................... 75

10.2 Appendix 2 – DSA Template_Form CF 0122 ................................................................. 76

10.3 Appendix 3 – Details on the Evolution of the Children's Automated Tracking System (CATS) in Kentucky ................................................................. 85

10.4 Appendix 4 – Data Governance Resources and Staffing ...................................... 87

10.5 Appendix 5 – Data Governance Processes .............................................................. 97
   10.5.1 Summary of Data Governance Process Flows ................................................... 97
   10.5.2 Manage Governance Framework ...................................................................... 98
      10.5.2.1 Assign stewardship to subject area data .................................................... 98
      10.5.2.2 Manage change to the data governance framework .................................... 99
   10.5.3 Manage Subject Area Data ............................................................................... 101
      10.5.3.1 Manage break-fix / maintenance / enhancement requests ........................ 101
      10.5.3.2 Manage new project requests .................................................................... 103
      10.5.3.3 Manage Data Pulls and Extract Requests ................................................. 105
   10.5.4 Manage Subject Area Data Quality .................................................................. 106
      10.5.4.1 Audit Subject Area Data ............................................................................. 106
      10.5.4.2 Resolve User Inquiries into Subject Area Data Quality .............................. 107

10.6 Appendix 6 – Data Acquisition Playbook .............................................................. 108
   10.6.1 Data Sharing and Data Acquisition Checklist: ................................................... 108
   10.6.2 Data Sharing and Data Acquisition Playbook Process Flows: .......................... 112
   10.6.3 Data Sharing and Data Acquisition Playbook Table: ...................................... 117
Revision History

<table>
<thead>
<tr>
<th>DATE</th>
<th>AUTHOR</th>
<th>VERSION</th>
<th>CHANGE REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/23/2016</td>
<td>North Highland</td>
<td>001</td>
<td>Initial draft</td>
</tr>
<tr>
<td>06/03/2016</td>
<td>North Highland</td>
<td>1.00</td>
<td>First draft submitted to OCW</td>
</tr>
<tr>
<td>07/11/2016</td>
<td>North Highland</td>
<td>1.02</td>
<td>Second draft with revisions based on DCF feedback.</td>
</tr>
<tr>
<td>07/20/2016</td>
<td>North Highland</td>
<td>2.00</td>
<td>Final Version</td>
</tr>
</tbody>
</table>

Quality Review

<table>
<thead>
<tr>
<th>NAME</th>
<th>ROLE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michiko Wolcott</td>
<td>Data Analytics Lead</td>
<td>06/03/2016</td>
</tr>
<tr>
<td>Tina Worley</td>
<td>Client Lead/Project Manager</td>
<td>06/03/2016</td>
</tr>
<tr>
<td>OCW</td>
<td>Client</td>
<td>06/20/2016</td>
</tr>
<tr>
<td>Tina Worley</td>
<td>Client Lead/Project Manager</td>
<td>07/15/2016</td>
</tr>
<tr>
<td>Michiko Wolcott</td>
<td>Data Analytics Lead</td>
<td>07/15/2016</td>
</tr>
<tr>
<td>Michiko Wolcott</td>
<td>Data Analytics Lead</td>
<td>07/19/2016</td>
</tr>
<tr>
<td>Tina Worley</td>
<td>Client Lead/Project Manager</td>
<td>07/20/2016</td>
</tr>
</tbody>
</table>
SECTION 1 INTRODUCTION AND EXECUTIVE SUMMARY

Based on the RFQ-#LJ070214 Statement of Work, Task Order #2, North Highland is providing the Department of Children and Families (DCF) with a data governance strategy, a Master Data Management Framework, and a Data Acquisition Playbook.

1.1 BACKGROUND AND OBJECTIVES

Section 409.997(1), Florida Statutes (2014), enacted by Chapter 2014-161 states the Department of Children and Families (DCF, Department), the Community-Based Care lead agencies (CBC),¹ and lead agencies' subcontractors share the responsibility for achieving the outcome goals specified in section 409.986(2), Florida Statutes (2014). These legislative actions created the Results-Oriented Accountability (ROA) Program, with the purpose of developing mechanisms to monitor and measure the use of Child Welfare resources, the quality, and amount of services and child and family outcomes.

During the FY14-15, a data analytics project was conducted for DCF to improve upon the limited analysis from the fall of 2013. Furthermore, the Office of Child Welfare (OCW) is currently working to implement elements of the Result-Oriented Accountability (ROA) Plan developed in FY14-15. Access and use of data, both internal and external, are critical not only to support the vision and objectives of the data analytics by the agency, but also to support the needs of the Results-Oriented Accountability Program that relies heavily on empirical evidence through the use of data.

The FY14-15 efforts identified a number of critical gaps with respect to the quality and management of data within and outside of DCF. Detail regarding these gaps can be found in the document “Data Analytics: Final Report on Data Discovery”. OCW has an increasing dependency on the quality of internal data, the ability to access external data in a timely manner, and the ability to ascertain the quality of the data once it is received. Without a foundational strategy, data governance, data management, and processes for acquiring data and enforcing data quality, the analytics and ROA efforts will be less effective, less meaningful, and potentially even misleading. One example of data issues is evident in FSFN, where duplicate persons is making it more difficult to link service delivery and abuse report histories to a single person record.

This report describes the framework for data strategy, data governance, master data management, and data sharing and acquisition, to begin addressing the gaps identified during the meetings and interviews held with DCF to document the current state of data governance. A summary of the gaps are:

¹ Section 409.986(3)(d), Florida Statutes (2014), defines a “Community-Based Care lead agency” as a single entity with which the Department has a contract for the provision of care for children in the child protection and Child Welfare system, in a community is no smaller than a county and no larger than two contiguous judicial circuits.
- There is no formal data governance committee or documented data governance processes.
- A metadata repository is needed, describing the data in DCF databases.
- Master data management IT infrastructure and tools need improvement.
- Data sharing agreement templates, as well as repeatable processes, are needed to make data sharing quicker and easier.

More detail is provided in Section 7 of this document.

A data strategy and data governance program concerns the overall management of the availability, usability, integrity, and security of the data employed in an initiative. Data management concerns the management of a single data source (such as FSFN), and master data management (MDM) extends this concept to multiple data files from disparate sources. Since data about a specific subject is often stored and supplicated in several disparate sources, making it difficult to know which version is correct and up to date. MDM is a comprehensive method of linking critical data to one file (a "master" file) that provides a common point of reference, building a single view of a given subject area. Proper MDM streamlines data sharing, the practice of making data owned by one organization available to others. Allowances and restrictions in how the data will be used, exchanged, and disposed are codified in a Data Sharing Agreement between the data owner and the data recipient. Data acquisition refers to the entire process of acquiring data through data sharing, including the methods of physically exchanging the data.

The main objectives of this document are to:

- Describe a data governance framework to support better communication between agencies and facilitate cross-agency data sharing.
- Describe best practices and procedures for data management and master data management (MDM).
- Present a Data Acquisition Playbook, a documentation of a step-by-step and repeatable process to identify and acquire data needed from external sources.
- Propose the organizational structure best suited to support the objective listed above.

1.2 CONNECTION TO THE RESULTS-ORIENTED ACCOUNTABILITY PROGRAM

This report aligns with ROA initiatives to:

- Create an analytics data strategy leading to consistency within DCF while addressing the need to incorporate data from sources outside of DCF.
- Establish data governance standards and procedures and propagate best approaches related to data usability, integrity, and security.
- Establish and implement master data management (MDM) procedures required to enable data quality, standardization, and stewardship responsibilities for child-centric data across the Child Welfare Community.
- Develop procedures and standards around intake of data from external sources (other state agencies, etc.) to increase data quality.
- Create a Data Acquisition Playbook incorporating lessons learned related to contracts, Data Use Agreements, Memoranda of Understanding, Data Sharing Agreements, etc., to speed the acquisition of data from new sources.
- Design and implement repeatable processes for data acquisition to make intake projects more efficient and effective.

### 1.3 SUMMARY OF RECOMMENDATIONS

A recent Florida Government Data Feasibility Study² found that twenty-seven (27) out of thirty-seven (37) state agencies surveyed identified privacy, confidentiality, security or contractual restrictions specific to their entity that restrict what data they can disclose. The processes and the requirements for data sharing and data access in Florida is currently determined by each agency or even by each division within each agency, creating a material barrier for any state initiative to become data-centric. An example of this is evident in obtaining vital statistics data from the Department of Health (DOH). Different organizations within DOH which provide different vital statistics data have different data sharing requirements. Since the data management and data sharing requirements and processes are not standardized, a statewide initiative toward a centralized data strategy and governance structure is recommended to facilitate the agility of the response to data needs across agencies, while protecting the integrity and security of the data shared.

However, North Highland recommends starting within DCF to reduce the risk of failure. Incremental steps should be taken to increase the likelihood of success in implementing a data strategy and data governance program while maintaining state-level support as the ultimate goal. The suggested approach is to apply the recommendations described in this document first within OCW or at the DCF level. This allows the approach to be refined, based on lessons learned, before trying to expand it on a larger scale. After success is demonstrated at that level, the effort can be expanded to a few key agencies. Once the processes are successfully adopted by the key agencies, expansion may be continued and statewide adoption may be sought. Many states realize that data is a valuable asset and that creating unified, high quality data at the state level allows the agencies to better serve its citizens.

The Policy and Services Research Data Center (PSRDC), located at the University of South Florida, already houses data files from several state agencies (e.g., Agency for Healthcare

---

² URL: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiGqMjBo7fNAhUK7iYKHTZqDckQfggmMAA&url=http%3A%2F%2Fwww.ast.myflorida.com%2Fdoc%2520library%2520%2F1%2520DEL6_GDFS_OUTLINE_FINAL_20150601.pdf&usg=AFQjCNH0PMkbCHgSVnIJcAtJPVqM3rv0Q
Administration, DCF, Department of Health). Once the data governance, data management, and MDM process are defined, OCW may consider leveraging PSRDC’s capabilities for OCW’s needs.

### 1.3.1 Data Governance

The data governance organization is responsible for the availability, usability, integrity, and security of the data utilized. It addresses the people and processes involved in the overall data strategy, with a set of defined procedures and a plan to execute them. The organizational structure that supports data governance should be made up of:

- A cross-functional Executive Steering Group of executive leaders
- A Data Governance Board that defines plans to execute the strategy
- Agency Function Data Stewards, responsible for the day-to-day work

In order for data management, master data management, and data sharing to succeed in a repeatable, sustainable way, a data governance organization should be in place to ensure that the direction and execution of the processes align with the strategic direction of the organizations involved. This is accomplished through the following steps:

1. Communicate the need for data governance and the changes it will bring. It is important to involve targeted organizations early through repetitive communication on progress and requests for feedback. Building the business case to justify the need is important for acceptance and approval.
2. Develop the charter that defines the business objectives and guiding principles. Once the business case is approved, documenting, communicating and getting acceptance of the data governance charter ensures that everyone understands the purpose of data governance. It also provides the focus point to ensure ongoing initiatives are aligned with the business objectives and guiding principles.
3. Establish the decision-making bodies and define policies and procedures once the charter is approved. When the policies and procedures are near completion, the architecture and tools needed to support data governance and master data management can be chosen and implemented.
4. Design, develop, and implement the processes to execute the policies and procedures, and monitor those processes for continuous improvement.

Properly implemented data governance should accelerate and simplify the data acquisition and management, rather than slow them down from additional layers of bureaucracy.

### 1.3.2 Data Management and Master Data Management

Planning and tool evaluation for master data management (MDM) should build upon the data governance and data management planning and foundation. Processes and procedures specific to MDM can be developed and tools can be evaluated that add capability to the existing data governance/data management foundation.
North Highland recommends starting by creating a single view of the person, the Person Golden Record (PGR), and including a child attribute to identify the children within the PGR. OCW can coordinate efforts with the Client Data Link project currently under way at DCF. Once the PGR business rules and automated processes are stable, relationships can be added to the child subset within the PGR, creating the Comprehensive Child View (CCV) hub. People and events related to child welfare can be associated to the CCV hub forming a 360-degree view of the child’s ecosystem. The CCV will show relationships of people that constitute the child’s family and household environment. Health and judicial information for the child and related people can all be associated to the child. The CCV model will be the basis of future Data Analytics and research supporting ROA.

The goal is to create a holistic view of child information to support a statewide collaborative child welfare community. Ideally, the CCV model should mature beyond OCW and DCF; the long-term vision is for all DCF Offices and state agencies impacting child welfare to leverage the CCV model and to share data to build a consistent view concerning the child.

1.3.3 DATA SHARING AND DATA ACQUISITION

The following figure describes a data sharing and a data acquisition maturity model, along with the drivers and facilitators influencing the maturity progression.

**Drivers**
- Valuing data as an insightful asset
- State legislators want to share data
- Agencies want to share data
- Lawyers are instructed to find ways to share

**Facilitators**
- Adhering to data exchange standards
- Service Oriented Architecture (SOA)
- Enterprise Service Bus (ESB)
- Development “accelerator” packages

![Figure 1-1 – Data Sharing Maturity Model](image-url)
OCW is currently at Level 1. In addition, there are currently no state level entities supporting data governance, data management, MDM, or data sharing. In order to move to a higher level of maturity, the following broad steps are recommended for each data sharing and acquisition opportunities:

1. Identify the specific data OCW needs, build the descriptive information that clearly define the data elements requested, and document the business case and justification for requesting the data.
2. Review existing Data Sharing Agreements (DSAs) in place to ensure they provide all the benefits and data access necessary. For additional data needs, identify the best data source organization for each category of data, start early communications with the organization to build trust and a collaborative environment, and help each data source organization understand the business objective behind the data need to gain empathy and support.
3. Work with the data source organization to identify any business process or technology modifications required, document the resources, schedule, and budget to accomplish the changes, and determine the funding source.
4. Review and modify the existing DSA templates to include all relevant topic areas. The DSA should be complete enough that, if additional data elements are needed in the future, they can be acquired through a simple addendum.
5. Once the data acquisition tasks are underway, work closely with the data sharing organization to establish the proper technology infrastructure and automated processes to facilitate data transmittal, notifications, profiling to ensure the data is in the expected format, and actions to take in case of unexpected results. As data sharing and data acquisition processes become more stable, the success should be communicated to include additional agencies to encourage following of the standard data sharing and data acquisition processes.

1.4 OVERARCHING VIEW

Defining and implementing an overarching data governance and strategy is not an easy endeavor; therefore it is important to re-visit the reason for doing so. OCW’s vision for ROA is:

“Child welfare communities have a unified or collaborative approach to provide quantifiable assurances demonstrating resources are used responsibly to ensure child and family outcomes are met and inform continued investment in the future of Florida’s children and families.”

The interrelated mission is:

“To develop an integrated, research-informed framework designed to inform communities, the child welfare system, and legislators on essential elements of child protection (Chapters 20, 39, and 409 Florida Statutes).”
OCW’s vision is focused on the child and family, and its mission is to provide the best information possible to the child welfare communities to ensure the best outcome possible for children and families. OCW realizes:

1. There is a need to be able to review and analyze outcomes with more breadth and depth.
2. There is a lack of evidence to support process measures that are valid and reliable.
3. Interventions are often implemented and replicated without a review to determine if the intervention is research-informed, or without evaluated to determine if the results are due to the intervention.
4. The outcomes have to be clearly defined and able to be measured.

A data analytics initiative was started to address these problems and support ROA. The quality of the analytics is only as good as the quality of the data going into the analytical models, hence the need for data governance, data management, and master data management. To derive useful information from the analytics, the data must be unified and managed with common data definitions and effective data sharing across the child welfare community.

The following figure shows an overarching view of the recommended DCF information management (IM) framework, supported by a tightly integrated series of people, processes, and technology focused on optimizing the value and use of information across the organization. The scope of the all-encompassing IM framework is only limited by the scale OCW and DCF desire to set. It may include organizations outside of DCF and eventually be implemented at the state level. More detail is provided in subsequent sections of this document. The questions posed will be answered by projects described in the Implementation Roadmap section of this document.
The framework has eight (8) components that fall into two major information management (IM) activities:

- **Data Acquisition and Management**
  - Master Data Management
  - Data Integration: Extract, Transform, Load (ETL)
  - Security and Privacy
  - Data Architecture

- **Data Exploration**
  - Metadata Management
  - Data Quality
  - Analytics

**Figure 1-2 – DCF Information Management Framework**
Furthermore, there are four (4) management areas that have an encompassing linkage over the above eight:

- Governance
- Program Management
- Technical Change and Communication Management
- Organizational Alignment

### 1.4.1 Core Components – Data Acquisition and Management

The following describes each core component within the Data Acquisition and Management activities within the framework.

- Master Data Management
  - How are key master data domains defined and managed?
    - Person
    - Client
    - Child
  - From what sources does data derive?
  - How is the data created and maintained?

- Data Integration
  - What ETL tools are in use to manage the transfer of data from sources to the data storage layer?
  - What ETL standards are in place?
  - What audit trail is in place as the data is moved, transformed, and stored?
  - What processes are in place for handling data issues with the ETL process?

- Security & Privacy
  - What database and report security is in place?
  - What tools are used to manage the security of information across the technology stack?
  - What is the process to ensure the privacy of personal data?

- Data Architecture
  - What is the overall architecture of the information flow and the warehouse and analytic data storage areas?
How is information organized in those layers?
What data models are utilized and is there an enterprise data model?
  Do diagrams exist?
What environments are available for development testing?
What tools and processes are used for configuration management and version control?

1.4.2 **CORE COMPONENTS – DATA EXPLORATION**

The following describes each core component within the Data Exploration Activities within the framework.

- **Metadata Management**
  - Is there a repository and if there is one, what tools are being used to store the metadata (e.g. data model, IM tool, ETL, etc.).
  - How does the organization handle business metadata, and technical metadata?
  - How readily available is metadata to report to users?

- **Data Quality**
  - How is data quality managed?
  - How is data quality validated?
  - How engaged is the business in owning the quality of the data?
  - How is the quality of data impacting the use and value of information?

- **Analytics**
  - What tools are used to meet analysis needs and how are they used?
  - How are users accessing information to perform analysis?
  - How is the organization deriving insights from data analysis?
  - How is the organization leveraging the analytical insights generated?

- **Reporting/Dashboards**
  - What business problems are being addressed by the reports?
  - What tools are utilized to create reports?
  - How are reports delivered or accessed?
  - How is the organization leveraging the insights generated from the reports?

1.4.3 **OVERARCHING MANAGEMENT AREAS**

- **Governance**
How are key data subject areas defined? How are key analytical areas and activities defined?
Are there enterprise-level definitions of key business data elements? Are there enterprise-level definitions of key analytical standards, policies, and practices?
How are definitional issues and discrepancies resolved?
What organization is in place to make the decisions to set in place the rules and process to govern the data? To govern analytical activities?
How are projects and requests for application functionality managed?
What is the process to develop rules and processes to ensure consistent and accurate data across systems?

Program Management
What structure and processes are in place to ensure project-level activity is supporting program goals?
How are projects approved and prioritized?
How are cross-project dependencies, risks, and issues managed?

Technical Change and Communication Management
How is the team organized to provide support of existing capability and development of new capability?
Who oversees the end-to-end data architecture? The end-to-end process of operationalizing analytics?
Is the team properly trained in data management? In analytical standards and best practices?
How does the group respond to changing business requirements while maximizing value and reducing incidents, disruption and re-work?
How are changes documented, approved, and shared?
How does the IM organization interface with other groups, internal and external to DCF?

Organizational Alignment
What is the IM organizational purpose?
How is the IM group organized?
What are the business facing roles?
How well are the roles defined within the IM organization?
How well does the group understand the Vision and Mission?
How do the strategies and initiatives among the areas of technology, data, and analytics align?
1.4.4 INFORMATION MANAGEMENT DELIVERY MODEL

Information management is an ongoing challenge due to the amount of change that occurs within an organization. A proper data governance strategy with enabling people, processes, and technology can mitigate many of the challenges faced with IM delivery models. The figure below shows how a good IM delivery model addresses data flow challenges. Data acquisition, governance, and management components of this model are described in more detail in subsequent sections of this document.

![DCF Information Management Delivery Model](image)

**Figure 1-3 – DCF Information Management Delivery Model**

Typical data flow challenges and how the IM delivery model can address these challenges are the following (refer to the numbers in Figure 1-3):

1. Disparate systems with limited integration often results in not knowing what data exists or how to get to it. The People aspects of the IM delivery model communicate and collaborate to understand and share data. Data standards are defined and enforced.
2. Lack of data governance and quality standards make it difficult to consistently manage information across the organization. The Process aspect ensures compliance with policies and procedures in a consistent, repeatable manner.

3. Data storage and exploration models, as well as technological tools, are often established independently based on individual departmental needs, contributing to the inability to get a unified view of the data. Coordinating all three aspects (people, processes, and technology) across the organization allows everyone to work together, with access to a unified view of the information needed to support the child welfare communities.

1.5 **SCOPE OF THIS DOCUMENT**

This document addresses the parts of the DCF Information Management Framework that relates to data as a raw material. This includes the Data Acquisition and Management activities (Master Data Management, Data Integration, Security and Privacy, Data Architecture) and two of the core components within the Data Exploration activities (Metadata Management, Data Quality), as well as the overarching management areas as they relate to these core components. The Analytics and Reporting/Dashboards components and their interactions with the overarching components are addressed in a separate document, "Foundational Processes for Analytics".
SECTION 2 CURRENT STATE IN FLORIDA

The following tasks were performed to understand the current state of data acquisition, data governance, and master data management in Florida’s child welfare:

1. Interviews/meetings were held with key personnel at OCW and DCF.
2. Existing documentation was reviewed.
3. Florida’s existing legislative and regulatory environment was researched, particularly concerning data sharing.
4. Existing Data Sharing Agreements (DSAs) and the processes supporting DSA creation were reviewed.

2.1 RESULTS FROM INTERVIEWS/MEETINGS

The results of the meetings are summarized here. Detailed meeting notes are available in Appendix 1.

While there is a need to acquire data from external sources, there is belief within OCW that the DCF should first focus on improving the quality of the data in the Florida Safe Families Network (FSFN), the primary operational system for child welfare in Florida. There is an initiative underway to re-educate the CBCs on FSFN capabilities and encourage the use of FSFN as the system of record for all child welfare work, whose consequence is expected to include improved data quality and content in FSFN.

The OCW Performance Management Unit accesses the FSFN data from the DCF data warehouse to create data marts to support federal reporting and compliance, day-to-day operations and executive reporting needs. Trend reports related to child protection investigations are also produced at the state, region, or circuit level using a commercial data visualization tool, Tableau, and the reports are posted to a public-facing website of the Florida’s Center for Child Welfare at the University of South Florida. While there is a committee supporting use of Tableau and the associated data, it is not a data governance committee. The Performance Management Unit has executed a number of DSAs, and there are existing templates. Recently, a DSA was executed in March 2016 with the Ounce of Prevention Fund of Florida to obtain data from Healthy Families Florida program.

Current DCF standards and/or processes supporting data governance, MDM, and data acquisition/data sharing was discussed with DCF. DCF explained that there was no specific IT activity around data governance; while there has been effort to link data across agencies in the past, legislative and regulatory restrictions terminated the project without completion.

At DCF, most data exchanged is outbound from the Office of Economic Self-Sufficiency\(^3\) and less frequently from FSFN. Each request is handled on a case-by-case basis, with each DSA requiring legislative justification. Once the DSA is executed, the data is exchanged through a

\(^3\) Its system, Automated Community Connection to Economic Self Sufficiency (ACCESS), houses the public assistance information.
point-to-point Secure File Transfer Protocol (SFTP) connection, and there are no formal processes or specific resources dedicated to MDM or data sharing. DCF IT desires to be involved in the MDM and data sharing processes to guide OCW down the right path. The Performance and Quality Management and DCF IT will collaborate to understand impact on ROA and data analytics initiatives and determine opportunities for working together.

Discussions with OCW have also confirmed that currently there is no formal structure supporting data governance or MDM, or any formal processes other than described in each DSA. The Performance Management Unit has created sets of code or scripts particular to the needs of each DSA, but they are not set up to process automatically. Minor configuration changes are needed as each data set is retrieved and the code is executed manually through completion. OCW is currently in the process of setting up an automated data exchange with the Agency for Health Care Administration (AHCA).

There is also no formal data transmittal or receipt acknowledgement process. None of the data OCW currently exchanges is supported by generic processes such as web services, and everything is handled on case-by-case and point-to-point. Furthermore, since there are no formal processes, there is no documentation other than the DSAs.

The DCF operating procedures and guidelines to set up and execute a DSA are documented in CFOP 50-26, Policy on Agreements Involving Data Sharing. Finalizing a DSA is considered to be a lengthy process involving agency workgroups and legal counsel. Each agency has its own process and sometimes its own DSA; if the agency’s process is not followed, data will not be received from that agency. The DCF Procurement Manager stated DCF once pursued a standard DSA in 2008; however, the efforts were halted, as it would have required changes in state and federal rules. It needs to be determined if this is still the case as part of the effort to develop a standard DSA template. This is one of the projects recommended in the implementation roadmap described in Section 8 of this document.

2.2 RESULTS FROM REVIEWING EXISTING DOCUMENTATION

The first document reviewed was CFOP 50-26, Policy on Agreements Involving Data Sharing. The document describes the need to protect the security, integrity, and confidentiality of client data. It requires the use of the web-based DCFTracker to track the review and approval of the draft DSA, as well as that every DSA be reviewed annually and expire after a maximum of three years. Any changes, modifications, or alterations must follow the same process.

OCW uses a standard template for the DSAs, “DSA Template_Form CF 0122”. A copy of the template is in Appendix 2. It requires the specific data elements be listed and describes the security and confidentiality mandates in sharing the data. Any DSA executed using this form
must be renewed annually. Any changes or modifications require the DSA to be re-executed unless specifically stipulated in the DSA.

There is also DSA template for use in sharing data between CBCs, DCF, and local school boards. While the use of this template is not required, it has the advantage of having been reviewed by DCF and the Florida Department of Education (DOE). Both agencies agree it is compliant with the Family Educational Right and Privacy Act (FERPA) and state child welfare confidentiality laws. A major stipulation is that OCW must obtain a parental release or court order for DOE to release medical or educational records about a child to OCW.

### 2.3 Existing Legislative and Regulatory Environment

The processes and the requirements for data sharing and data access is determined by each agency or even to each division within each agency, based on each group’s interpretation of the legislation and regulations around data security and confidentiality. There are general rules which may be at the state or federal level, and there are rules that are agency-specific. There is a perception within DCF that the interpretation under which each group works may be based on outdated rules or may not have been correct in the first place. CFOP 50-26 refers to several other sections of Florida Administrative Code and Florida statutes listed and highlighted below.

- **Florida Administrative Code Chapters 71A-1** documents a framework of information security best practices for state agencies in order to safeguard the confidentiality, integrity, and availability of Florida government data and information technology resources. Florida Administrative Code Chapters 71A-2 defines minimum security standards for the protection of state information resources. Neither of the Codes have language specific to data governance or MDM. 71A-1 refers to data sharing, stating that “for systems containing exempt, or confidential and exempt data, each agency shall ensure written agreements and procedures are in place to ensure proper security for sharing, handling or storing confidential data with entities outside the agency.”

- **Florida Statute Chapter 39** describes proceedings relating to children. Relating to data, Chapter 39 describes the collection of data needed for service management, compliance monitoring, and performance reporting, but it does not contain anything specific about data governance, MDM or DSAs. Section 39.908 does stipulate that information received by the department is confidential and exempt from the provisions of s.119.07(1)⁵. Information about domestic violence clients cannot be disclosed without written consent of the client except by court order or in certain specifically listed emergency situations.

- **Florida Statute Chapter 119** focuses on public records and public records exemptions. For the Department of Health (DOH), it specifically states that any personal identifying information (PII), personal health information (PHI), or eligibility for health related

---


41T Florida Department of Children and Families – 41T Data Governance and Strategy

Deliverable #4

Office of Child Welfare
service is not allowed without the written consent of the individual, or the individual’s legally authorized representative in case of an emergency or by a court order. Data may be released for research but must be de-identified.

- Florida Statute Chapter 812 deals with theft robbery and related crimes. It does refer to data communications/piracy, but does not involve data governance, MDM, or data sharing.
- Florida Statute Chapter 815 concerns computer-related crimes. It does not involve data governance, MDM, or data sharing, other than to say that the unauthorized acquisition of data is a crime.
- Florida Statute Chapter 839 concerns offenses by public officers and employees. It does not involve data governance, MDM, or data sharing.
- Florida Statute Chapter 877 deals with miscellaneous crimes. The only stipulation regarding data is the prohibition of using any data that identified the victim of a hate crime. It does not involve data governance, MDM, or data sharing.

2.4 EXISTING DATA SHARING AGREEMENTS AND SUPPORTING PROCESSES

The fundamental challenge in acquiring data from other agencies is the fact that there is little standard among the agencies. Each agency has its own processes and requirements for data sharing, and some agencies have different processes and requirements within the same agency for each division and/or data source. To further complicate the matter, some data sources may not have formal standards, processes, or requirements for data sharing, and for some others, while such formal requirements exist, much is subject to interpretation and there is no general consensus on the exact requirements and processes.

The overall process to request and receive approval for data sharing across agencies requires a long time from the identification of the initial request for information, initial contact, to approval. Some request and approval processes can take several weeks, and in some cases, simply identifying the right contacts and actually making those initial contacts can be a lengthy process in itself.

A number of DSAs have been executed by DCF that are related to the child welfare data analytics projects in FY14-15 and FY15-16. They include DSAs with the Department of Health Bureau of Vital Statistics, the Ounce of Prevention Fund Florida, and North Highland. The current DSA with Vital Statistics does not provide all the data needed for ROA and data analysis and should to be amended and re-executed. There was also a communication to agencies memorandum from DCF to heads of agencies originally identified as the owners of priority data sources (the Department of Health, the Agency for Health Care Administration, and the Florida Department of Law Enforcement).

Further research uncovered other agreements that involve data sharing. From the Florida’s Center for Child Welfare website – DCF Interagency and Other Agreements:
1. “The Interagency Agreement between DCF and DOH Sexual Abuse Treatment Program (2015)” describes the agreement to share client specific data between the two agencies. It also describes linking the FSFN and DOH information systems.

2. “Interagency Agreement between DJJ and DCF - Data Sharing (2015)” focuses on data sharing guidelines to allow for sharing of research data to promote enhanced decision support, data quality, and services. This agreement stipulates that DCF will share individually identifiable records with DJJ, and DJJ will share individually identifiable records with DCF following Florida statutes 985.04 and 943.05. These statutes suggest that data may be shared as long as the agency with which it is shared keeps it confidential.

3. “Memorandum of Understanding Between the Florida DCF and Agency for Health Care Administration (2012)” allows Medicaid eligibility and claims payment data to be shared.

4. “Working Agreement Between DCF, SA/MH and CBCs (2004)” allows for coordinated and collaborative working agreements. It also allows for shared case management and shared information between the groups after securing the appropriate consent.

It may be possible to build upon these existing DSAs to achieve longer term OCW goals. Another possible consideration is to leverage the Florida Health Information Exchange to obtain a broader view of an individual’s health information.
SECTION 3  LESSONS LEARNED

The content in this section is based on the Data Governance Strategy Facilitated Session held on April 01, 2016. First, the documentation of the current environment was reviewed and verified. The group agreed that, while formal data governance and MDM processes are not defined for external data management, there are process in place for internal data management, i.e. MDM and data exchange between applications and divisions within DCF.

The DCF CIO stated it is important the scope of the data governance/MDM discussion be clearly defined. He explained there were good processes in place for operational but not analytical data management and exchange, which are generally ad hoc in nature. The group agreed that the scope and discussion would focus on analytical data governance and MDM, starting at the OCW level, then moving to DCF and potentially beyond.

With that in mind, a discussion started on lessons learned and the pain points in the current OCW/DCF analytical data governance, MDM and data exchange processes.

- **Data quality**: OCW, and DCF in general, need a better understanding of the quality of the data in the various data stores used in business operations and decision-making. Currently, data is fragmented and duplicated, leading to inconsistencies. While various definitions of data quality exist, they generally concern whether the data is fit for intended uses in operations, decision-making and planning. Aspects of data quality include:
  - Completeness: The proportion of stored data against the potential of "100% complete."
  - Uniqueness: That nothing is recorded more than once based upon how the data objects are identified.
  - Timeliness: The degree to which data represents reality from the required point in time.
  - Validity: Conformity to the syntax (format, type, range) of its definition.
  - Accuracy: The degree to which data correctly describes the object or event being described.
  - Consistency: The absence of difference when comparing two or more representations of the same object or event.

- **Data timeliness**: Timeliness can be measured as the time between when data is expected and when they are readily available for use. Data timeliness is one of the most frequent data quality dimensions that must be managed. Data may be accurate and complete at the time of data entry, but the real-world construct the data refers to may change over time, making the same data inaccurate and incomplete. There is a need to determine and prioritize the timeliness needs of each data category.

- **Data categorization**: OCW can gain a better understanding of the data it has and the data it needs by sorting and grouping data into various types and distinct classes.
according to data set requirements for various objectives. Data categorization will allow OCW to be more specific about the data elements being requested, moving away from requesting all the data available in an external data file. It will also allow OCW to gain a better understanding of the legislative and security impacts concerning the data and help determine the best source of data and aid in the prioritization of data acquisition.

- **Document the employee subject matter expertise that is currently undocumented**: Losing the expertise and experience of key employees could significantly reduce efficiency, resulting in costly mistakes, unexpected quality problems, or significant disruptions in services and/or performance. Capturing and sharing critical knowledge and expertise allow those who remain to continue providing quality service.

- **IT infrastructure and tools**: The appropriate infrastructure and tools are not in place to support MDM and data exchange.
SECTION 4  MODELS USED BY OTHER STATES AND AT THE FEDERAL LEVEL

Deliberate, actionable, and effective data management process and practice has become a top of mind issue for public entities including federal, state, and local agencies. The following excerpt from a 2012 Information week article highlights the need:

In a just released report on the role of big data in state government, the National Association of State Chief Information Officers (NASCIO) is advising its members to develop an enterprise architecture and data governance policies to maximize the potential of the information their state agencies generate. "The challenge is that many state government agencies are still being run as islands of information versus members of a single state government enterprise," the report states. "The result is state government is not fully exploiting the data it has at hand." (Information Week, 2012)

It behooves state agencies to take this recommendation seriously, and begin to manage data at an enterprise (state) level as an asset. The following sections highlight how some other states are maturing in their efforts to do just that. The states were chosen for the following reasons:

1. Colorado: Appeared to be a progressive leader in data strategy.
2. Kentucky: Passed a law to share citizen data across all agencies, which has accelerated their data strategy.
3. Tennesee: DCF learned of a potential data sharing agreement initiatives in that state.
4. Virginia: North Highland is familiar with its data strategy initiatives and its unique approach to the data sharing agreements.

4.1 COLORADO

At the time of this document, Colorado is one of four states that employs a Chief Data Officer, along with Texas, New Jersey, and Utah. California may become the fifth state pending legislation. Since 2007, The Governor's Office of Information Technology (OIT) in the state of Colorado has produced a groundbreaking and progressive agenda for information sharing and information technology management. OIT has focused on agile application and service delivery with a strong emphasis on data quality. The Colorado Data Strategy ensures that state government policymakers and knowledge workers have the data and information they need to do their work. The “businessization6” of government requires a disciplined approach to managing data and information resources. Outcomes gained include:

- Dismantling data silos.

---

Data Governance

Since 2007, the Governor’s Office of Information Technology (OIT) has produced a groundbreaking and progressive agenda for information sharing and information technology management in the State of Colorado. It is recognized by both the Governor and the Colorado General Assembly that in order to more effectively serve citizens, improve the efficiency and effectiveness of state government, and inform policymaking, a strong program of information sharing is required across all lines of agency the state serves, as illustrated below:


Figure 4-1 – Realizing Benefits from an Effective Data Strategy for Colorado
OIT’s focus on agile application and service delivery means that strong concentration and emphasis on the underlying data required for employees, agencies, legislators, and others to do their work must be a top priority.

Specifically, a progressive data management strategy can provide the following benefits across the enterprise:

- **Education** - Ensures that a seamless education system from pre-school to graduate school is preparing our young people for the demands of the 21st Century by linking records over time (PreK-20), analyzing performance, and studying educational effectiveness.

- **Social Services** – Creates means to capture data once – regardless of point of entry into the state system - about a child, youth or family, and use that data across multiple state service programs to directly certify them for supplemental or additional services based on child or family eligibility. This program has a twofold benefit: ensuring that all children and families receive the benefits that they may not otherwise have applied for, and reducing fraudulent claims against the system by comparing the records.

- **eGovernment Services** – Provides single-sign on for citizens and agencies to have access to all of their current state account information (driver information, vehicle registration, tax information, benefits, etc.) through one portal. Digital signature services would be available to complete transactions electronically, end-to-end, with the state. The state would also be able to provide services such as address change that are completed once and shared with all agencies with which the individual does agency.

- **Workforce and Economic Development** – Creates strategic, targeted, and systemic responses to economic conditions and labor market changes. Information sharing can help support the development of timely, accurate information to identify key industries, examine the state of regional economies, explore the root causes of skills gaps, and promote strategic planning that addresses the needs of workers and employers alike.

- **Law Enforcement** – Improves state and community security and safety postures. All major reviews of the nation’s response to the terrorist attacks of 9/11 maintain that integrated information technology and improved information sharing across agencies at all levels of government are vital to an effective homeland security strategy.

- **Policymaking** - Helps lawmakers and policymakers answer questions and predict program results to help ensure the best use of limited State resources and effectiveness of State programs.

OIT is the central authority for all information technology (IT) systems, resources, and budget in the state of Colorado, and is authorized to set standards, policies, and guidelines for how those IT assets operate, communicate, and are managed. OIT has been examining the issue of data management for two years, bringing together cross-functional, multi-agency teams, interviewing stakeholders, benchmarking other states, and doing critical research to determine the most effective way to establish a new data management program in an environment of historically siloed agencies and systems.
The Government Data Advisory Board (GDAB), seated in August 2009, is a multi-agency central governance authority, comprised of representatives of 12 state agencies, local governments, non-governmental organizations and research institutes, and a wide variety of education stakeholders. The GDAB’s mission is to provide guidance and recommendations on how the state should govern and manage data and data management systems to improve the efficiency and effectiveness of state government, citizen service delivery, and policymaking. The GDAB is one of the very few such Boards in any state in the country, established in legislation and appointed by the Governor, to provide the central governing structure for enterprise data sharing initiatives. Additionally, a Data Steward Action Council (DSAC) is being established to formalize and organize the stewardship activities and processes enterprise-wide based on information subject areas. The DSAC will also create a common baseline of information, a statewide foundation for data sharing, information discovery, and future architectures.

The State of Colorado’s vision is to be one of the most innovative, admired organizations for our approach to data governance and enterprise data management.

The mission for enterprise data management is to foster collaboration, innovation, and agility in delivering government services to the citizens of Colorado through the seamless, efficient, strategic exchange of core data sets resulting in increased effectiveness of government operations. Figure 4-2 shows the alignment of the vision and mission with the program’s strategic objectives and key initiatives.
4.1.2 **MASTER DATA MANAGEMENT**

Colorado is taking a very proactive, best-practice view regarding master data management as noted by this excerpt from their data strategy document:

> **MDM is a modern approach that provides data management and specialty services out of the box designed to deal with the data fragmentation and data quality issue. It also provides a different approach with regard to data integration. Traditionally data integration is done on a point-to-point basis creating a tremendous complexity that increases exponentially with the number of systems that are participating in the integration. MDM leverages modern**
service oriented architecture (SOA) integrations based on a hub and spoke approach that reduces the integration efforts. MDM takes advantage of the canonical objects that are the common representation of the citizen attributes across all the parties involved in the integration. Due to the nature of the systems the concept of “citizen” will vary depending on the intent the system was created. The concept of “citizen” for a call center application is different from an HR system or from a financial system.

As an example, there is a need to define “citizen” so there is a common set of attributes across all the system within the state and that is the canonical object. The benefits of the MDM solution reside in the ability to consolidate, clean and share and standardize citizen information across these heterogeneous Agency systems throughout the state and it does have a substantial impact in the operations, the services and downstream analytics and reporting. MDM can deliver the right data to an analytics framework. MDM can deliver cross reference IDs across agencies for a particular citizen.

MDM provides services with the ability to:

- **Consolidate Information** into one master repository from disparate systems and organizational units; this step involves the identification and cross-referencing of people by their external ids or their representation in other systems. The initial creation of a best version is when the unique ID (Colorado Unique Personal ID, CUPID) is created. It also involves the storing of all of the source information, known as the Source Data History, so that a record of where and how the best version or golden record was created. Basically, it is a historical view of all the merges that occurred in creating the best version so that a data steward can go back and recreate the steps that led to the current best version. Survivorship entails the weighting of certain fields by source in the creation of the golden record. For example, the call center would have a higher confidence level for the address fields than the web site because call center personnel validate the person’s address by asking, “Do you still live at 123 Elm Street?”

- **Cleanse and Enrich** data centrally, applying the various data quality components to the information.

- **Distribute Data** as a single point of truth for a consistent enterprise view, sharing the information either in batch or just-in-time publishing.

- **Leverage Master Data** to service consuming applications, enterprise agency processes, and decision support systems in support of key Agency and state level agency processes.

### 4.1.3 DATA SHARING

Colorado has acknowledged that the historical methods of data sharing have not been effective or efficient and have taken steps in both policy and technology to improve data sharing processes. To that end, the Legislature has passed a series of bills over the past few years to address these issues, including HB 08-1364 (Interdepartmental Data Protocol) and HB 09-1285 (Government Data Advisory Board).
The Data Protocol Development Council established under HB 08-1364 provided strong recommendations and guidance on establishing such a program. The mission of the Council was to provide guidance, policies, and procedures for implementing a data sharing architecture across the state enterprise to achieve the data sharing goals and objectives of HB-1364. Two of the primary recommendations of the Council were to establish a formal enterprise architecture office and data management program with OIT and to establish a central governance authority to provide leadership and oversight for data sharing and data management activities. The central governance authority, the Government Data Advisory Board (GDAB), was established in legislation in 2009 (HB 09-1285).

The GDAB is a multi-agency central governance authority, comprised of representatives of 12 state agencies, local governments, non-governmental organizations and research institutes, and a wide variety of education stakeholders. The GDAB's mission is to provide guidance and recommendations on how the state should govern and manage data and data management systems to improve the efficiency and effectiveness of state government, citizen service delivery, and policy-making. The GDAB is one of the very few such Boards in any state in the country, established in legislation and appointed by the Governor, to provide the central governing structure for enterprise data sharing initiatives.

4.2 Kentucky

Kentucky was chosen as a state to research because it has a law supporting sharing information across state agencies as stated in Kentucky Revised Statutes (KRS) 61.878 (5). This statute allows for the exchange of public records or sharing of information between public agencies when the exchange is serving a legitimate governmental need or is necessary in the performance of a legitimate government function.

4.2.1 Data Governance

Kentucky has moved away from an agency specific view of data to a statewide or enterprise view. To transition from a tactical approach on data use to a strategic role, Kentucky changed its views on data ownership and access. Kentucky realized that a holistic view in a timely manner is key and essential for improved results when making economic development, budget, and policy decisions. To support this effort, the Commonwealth Office of Technology created the Kentucky Enterprise Data Architecture (KEDA) initiative. The Commissioner of the Commonwealth Office of Technology (who also serves as the Commonwealth’s Chief Information Officer) has direct responsibility for KEDA.

An Interagency Task Force (ITF) provides direction and approval of the KEDA strategy. This group also serves in a strategic capacity as the Executive Steering Committee of the initiative. Governance resides with the Commonwealth Office of Technology and the Enterprise Architecture Standards Committee (EASC). These two work together to establish data architecture policy and standards for adherence throughout the Executive Branch of state government. Where necessary, a subcommittee of technical experts from a representative
segment of EASC member agencies are called upon to further clarify issues and propose standards.

Data Stewardship is the responsibility of each agency. Data Stewards are established within each of the business areas. These individuals will have primary responsibility for a data subject area across business processes and applications to assure the quality of data are enforced and enterprise standards are followed. Their primary role will be to understand the data, business rules, and toolsets in order to properly define the data and monitor its quality, accuracy, consistency, security, and privacy.

4.2.2 MASTER DATA MANAGEMENT

MDM strategy, processes, structure are the responsibility of KEDA. Kentucky’s goals for MDM is to:

- **Improve Data Interoperability**: Facilitate the elimination of point-to-point architecture and the increased proliferation of enterprise-based systems.
- **Improve Data Reliability**: Facilitate agency level comprehension of standardized data elements and the ability to communicate within and between agencies about data with a clear understanding of its meaning.
- **Decrease Redundancy**: Facilitate the elimination of redundant data, decreasing Commonwealth hardware, software and support resource costs.
- **Promote Reusability**: Facilitate reduction in logical and physical database design time by utilization of established standards. Standardized interfaces will also decrease time-to-production for system development.

The role of administering the MDM toolsets resides within the Commonwealth Office of Technology. Some tools are administered within the Office of Application Development while others are administered within the Office of Infrastructure Services, depending on functional area of support (e.g. Data Profile vs. DBA).

Kentucky has established the Enterprise Common Data Framework (ECDF), a library of components for the most widely and commonly used types of data across the Executive Branch of Kentucky State Government. The framework for these Common Data Elements consists of the following:

- Common Data Models
- Data Definition Language (DDL) for data structure creation
- Class Objects to support the Data Model

The purpose of this is to make data integration efforts within an agency and across agencies more efficient and improve data quality.
4.2.3 **DATA SHARING**

While federal privacy and confidentiality laws must still be considered, KRS 61.878 (5) makes it much easier for agencies within Kentucky to launch data sharing initiatives. The Kentucky Court of Justice Family and Juvenile Services division has developed the Children's Automated Tracking System (CATS), a single source of case information for the Administrative Office of the Courts (AOC), judges, Citizen Foster Care Review Boards (CRCRBs), and the Department of Community-Based Services (DCBS) staff. The workgroup overseeing CATS recently partnered with the Department for Behavioral Health, Developmental, and Intellectual Disabilities (DBHDID) to ensure that services are not duplicated and data are collected and shared in a manner that benefits all systems. More information about the evolution of CATS can be found in Appendix 3.

4.3 **TENNESSEE**

Tennessee, like many other states, is predominantly agency driven in data management and strategy. While they have created the multi-discipline, multi-department Information Systems Council (ISC), their focus is not narrow and includes all technology and information disciplines. Some agencies, particularly related to education and healthcare, have implemented some best practice objectives to accomplish their mandated goals.

4.3.1 **DATA GOVERNANCE**

Tennessee has an inventory of IT governance policies, mostly dating back to the mid 1990’s, with some minor revisions, related to data management and strategy. *ISC Policy 10.00 – Data Resource Management* outlines the following high-level objectives.

- Plan and promote the effective and efficient sharing and usage of data to support State Government.
- Ensure personnel have access to the data they need to perform their job functions.
- Promote the understanding and accessibility of the State data resources.
- Facilitate ad hoc access and reporting of data maintained in relational databases.
- Ensure data resources will be shared among systems (applications, users, agencies).
- Ensure data redundancy is minimized and managed.
- Ensure data will be precisely and consistently defined (i.e. that standards exist and are enforced).
- Manage the data life cycle independent of the application system life cycle.

While the policy lists the key goals related to governance and interoperability, there is little content related to tactical implementation, organization, or process. Each agency is tasked with implementing the policies at the agency level with no requirement for cross agency harmonization or reconciliation of people, process, or technology.
4.3.2 MASTER DATA MANAGEMENT

Tennessee has not published any publicly available information regarding their policies or initiatives related to master data or MDM projects at the state level. The state references its Master Provider Index and Master Facility Indexes related to its work in Health Information Technology (HIT) and Health Information Exchange (HIE). The Tennessee Department of Human Services (TDHS) enterprise systems modernization vision includes MDM as a major objective to include master data for person, provider, and location.

4.3.3 DATA SHARING

Tennessee ISC policy 10.00 – Data Resource Management promotes data sharing, but provides little to no detail on the specifics at the state level. Individual agencies are encouraged to plan and promote the effective and efficient sharing and usage of data to support state government.

eHealth initiatives and Health Information Exchange (HIE) in the state have prompted best practice data sharing and exchange policies at the agency level. Legislation was passed in 2015 (HB0233/SB1331) mandating that the Commissioner of Health implement policies ensuring secure compliant exchange of all HIPAA category data. Additionally, some agencies are wrapping all sensitive and PII category data in a Continuous Quality Improvement (CQI) program to add repeatable rigor to data collaboration and exchange. For example, the Department of Child Safety (DCS) has implemented a CQI process to ensure data is shared effectively and securely with appropriate agencies and other outside consumers of their data.

4.4 VIRGINIA

Virginia was chosen as a state to research because of it has a well-structured enterprise data governance and data management strategy. It also has a unique approach to developing DSAs.

Data assets, at the state level, are administered under the Enterprise Information Architecture (EIA) function within the Virginia Information Technology Agency (VITA). Data are administered at the state level, but the decision-making authority regarding the data itself remains with the state agencies. State agencies control the data within the agency domain.

An important factor in Virginia’s EIA is the level of authority imposed. Guidance, standards, processes, and tools are available to any of the state agencies, but it is not required. VITA espouses the benefits of using all the resources available as accelerators for data governance, MDM, and data sharing, but agencies can do this all their own. VITA allocates a prorated portion of the budget across all agencies actually utilizing EIA.

4.4.1 DATA GOVERNANCE

Data governance represents the strategy dimension of the EIA program, with clearly defined objectives cascading from the enterprise to the Agency and program level. Key factors within
the enterprise data governance domain include strategic direction, institutional arrangements, agency relationships, and administrative functions necessary for aligning the Commonwealth’s EIA with the Business Architecture.

There is data governance oversight at the state level, but actual control flows down to the agencies and programs within agencies. There is a central data governance organization with executive sponsorship and guidance from a group of secretariat and agency leaders. Members may move in and out of the oversight committee, depending on the agency level of involvement. State level guidance provides data strategy a well-defined policy, standards, and guidelines. This is driven by relationships among data stewards at the enterprise, agency, and program level, with feedback loops in place at every level to support continuous improvement.

4.4.2 MASTER DATA MANAGEMENT

In Virginia, MDM is referred to as the EIA Data Asset Management Domain. The Data Asset Management Domain focuses on the development, implementation, and maintenance of an enterprise-level inventory of the Commonwealth’s data assets. It features high-level metadata and related data documentation at the Secretariat, Agency and program level. The metadata inventory is structured based on a detailed taxonomy with subject-area and information-class categorization. The inventory is housed in a central metadata repository, with data assets mapped to adopted enterprise data standards. This asset mapping supports gap analysis and identification of areas requiring new enterprise data standards.

The EIA Data Standards Domain focuses on the establishment and maintenance of adopted Commonwealth data standards. This includes standards for data management, data storage, data exchange, information architecture, messaging and implementation guides. It fosters semantic interoperability across Virginia based on enterprise agreements on common data/attribute definitions, specifications and vocabularies for data/information assets. This group is responsible for publishing and maintaining enterprise data standards in the EA Standards Repository.

The Data Standards group emphasizes using external standards maintained by national/international Standard Development Organizations. The group develops and publishes these standards to reinforce strategies for data quality and integrity. They are maintained in a central repository with resources to support agency capacity building and compliance.

VITA also supports a set of tools to implement MDM, available for agency use at a cost based on utilization.

4.4.3 DATA SHARING

Virginia refers to this as the EIA Data Sharing Domain within the EA. The EIA Data Sharing Domain promotes the formation of a Commonwealth-wide trust framework to enable the exchange of information across organizational domains and source data systems. The trust framework will be modeled on the Federal Data Utilization and Reciprocal Support Agreement (DURSA) and consist of requisite legal agreements. The trust framework and implementing
legal agreements will enforce compliance with all security, privacy, consent, and authorization codified in applicable law.

Secretariats from several Virginia agencies formed the Secretarial Committee on Data Sharing (SCDS). The SCDS mission centered on identifying opportunities and constraints for an enterprise data-sharing agreement and recommending action steps needed to establish such an agreement for participating agencies.

SCDS recommendations include the following:

1. Issue an executive-level directive to COV agencies to establish a trust-agreement framework in support of enterprise data sharing.
2. Form a governance committee of executive staff, data owners, data stewards, business leads, technical leads, legal staff, security staff and other representatives from COV agencies to develop, implement, and maintain a trust-agreement framework for the Commonwealth.
3. Identify applicable legal, regulatory and policy constraints impacting data sharing and orient the trust-agreement framework to comply with applicable requirements.
4. Identify legal requirements for informed consent and authorization and design the trust-agreement framework to comply with these requirements.
5. Develop policies, standards, guidelines and procedures to govern the operations, onboarding, maintenance, breach resolution and certification processes associated with the implementation of the trust-agreement framework.

Virginia has devised the Enhanced Memorandum of Understanding (eMOU) to support data sharing:

- A data sharing “accelerator”, approved by the state Office of the Attorney General that 80% or more of the DSA work in a “boiler plate” working document
- Enterprise data-sharing built on a solid trust framework and legal agreements modeled on the Federal DURSA
- Security, privacy, consent and authorization addressed based on applicable law
- Interoperability with other states and national information exchanges

The eMOU is supporting data sharing between a growing list of agencies in Virginia including:

- Department of Health (VDH)
- Department of Justice (DOJ)
- Department of Social Services
- Department of Medical Assistance Services
- Department of Behavioral Health and Disability Services
- Department of Healthcare Providers
SECTION 5  RECOMMENDED STATE

5.1  DATA GOVERNANCE

5.1.1  FUNCTIONAL ORGANIZATION AND GOVERNANCE

The following organizational framework is recommended for OCW/DCF. This model integrates people, process, and technology to greatly enhance the value of information assets used by DCF and sister agencies and departments.

- Cross Functional Executive Members
- Define strategic direction for Data Initiatives
- Final Decision for Unresolved or Escalated issues
- Govern balance between local needs and strategic agency objectives
- Define Roles and Responsibilities

- Defines corporate system data standards and ensures compliance
- Meets on a regular basis to discuss the status and direction of the data governance program
- Institutes corporate system governance policies that align with strategic agency objectives
- Escalates to the ESG any cross-team issues that it cannot resolve
- Subject Area, Cross-Enterprise Role
  - Drives common enterprise data definitions and evolution across agency units under the direction of the ESG
  - Reconciles definitions of data
- agency Function, Cross-Subject Area Role
  - Drives development of agency function specific data definition extensions
  - Prioritizes and sets direction for data initiatives
  - Facilitates communications across functional area

* SME’s defined as part of project and will change based on client need

Figure 5-1 – Data Governance Organizational Framework

5.1.2  DATA GOVERNANCE EXECUTION MODEL

While there are several models for executing data governance functionally, given the constraints, priorities, and agency-centric thought related to the state of Florida and state government in general, the subject-area based execution model is recommended for DCF and OCW. Required activity can be accelerated in that this model usually allows for clear up-front ownership boundaries and decision rights while following best practice standards and processes that are scalable at the agency, department, and state levels. In the Subject Area Model, a data steward owns and manages a discrete data subject area.
The benefits of a data subject area oriented stewardship model include:

- Ownership boundaries that are usually clear.
- The data steward’s knowledge of the accompanying agency rules and usage environments for her data subject area are likely to increase over time.
- This model is often easy to gain acceptance: someone needs to own customer data.
- Most agency personnel would agree to this model, as it is easy to understand.

The risks of data subject area stewardship include:

- Measuring the data steward usually focuses on data quality improvements at the expense of broader agency benefits like customer retention or consolidated item master.
- The potential size and scope of a given data domain – across multiple organizations, processes, and agency applications – may make finding qualified data stewards challenging.
- Subject-area data stewardship can be fraught with political landmines as resources refuse to cede control.
- It can be difficult to tie the data steward to actual agency initiatives since the data steward can only be as effective as the agency initiatives it supports. Therefore, this model calls for tested relationship-building skills.

Figure 5-2 – Subject Area Data Governance Model
5.1.3 **RECOMMENDED STEPS TO IMPLEMENT DATA GOVERNANCE**

1. **The business need for data governance needs to be socialized, at least within DCF.**

   The goal is to obtain agreement that the benefits of proper data governance outweigh the costs. Decisions regarding data management should be made by a group representing all DCF departments, aligning the data governance objectives with the overall Agency goals and drivers. Costs and a funding strategy should be established to ensure that data governance is a sustainable endeavor.

2. **The Data Governance Framework should be defined and documented, clearly defining its objective and purpose.**

   The outcome of this recommendation is a document analogous to a project charter. It will describe the data governance program objectives and guiding principles. The expectations and goals will be defined, along with the metrics and Key Performance Indicators (KPIs) to measure success. It will also include an organizational structure defining management and oversight roles and responsibilities. The Data Governance Framework will describe the data governance business structure to individuals outside of OCW so everyone has a common understanding of what data governance will accomplish.

3. **Policies and procedures should be documented, clearly describing the planned operational aspects of data governance.**

   Roles, responsibilities, and decision rights below the executive strategic levels should be defined to ensure strategic objectives are executed. Best practices and standards should be established for effective data management that ensures data quality, integrity, and protection.

4. **The functions needed to implement policies and procedures should be designed.**

   The data management architecture and processes, from both the business and the IT perspective, should be developed and made operational. People, processes, and technology must be considered in this step. Also, the entire data life cycle must be taken into account, from intake until it is no longer used.

5. **Once data governance is operational, continuously monitor, measure, and revise the processes.**

   Metrics and KPIs should be monitored to ensure the operation is accomplishing the data governance goals and objectives. Success should be communicated early and often, inside and outside the data governance organization to encourage acceptance of the program. Areas for improvement should also be communicated to promote transparency and trust.
5.2 MASTER DATA MANAGEMENT

North Highland recommends pursuing an ongoing best-practice strategy related to master data management practice, process, and technology. MDM will be a key component of realizing the stated DCF goals of quickly arming front-line DCF analysts and caseworkers with relevant and timely information to ensure child safety and welfare. North Highland recommends starting by creating a single view of the person, the Person Golden Record (PGR), and including a child attribute to identify the children within the PGR. OCW can coordinate efforts with the Client Data Link project currently under way at DCF. Once the PGR business rules and automated processes are stable, relationships can be added to the child subset within the PGR, creating the Comprehensive Child View (CCV) hub. People and events related to child welfare can be associated to the CCV hub forming a 360-degree view of the child’s ecosystem. The CCV will show relationships of people that constitute the child’s family and household environment. Health and judicial information for the child and related people can all be associated to the child. The CCV model will be the basis of future Data Analytics and research supporting ROA. The figure below is illustrative of a conceptual high-level master data process for developing an ongoing comprehensive view of child information from multiple key data sources.

What do we mean by Centralized Child View?

![Centralized Child View Diagram]

Figure 5-3 – Centralized Child View

Once in place, an ongoing, comprehensive, and mature MDM process, coupled with sound data governance, becomes the engine that drives data quality, integrity, and timely information.
at DCF/OCW. The figure below reinforces the important notion that people, process, and technology can be integrated in a holistic ecosystem to benefit all users of important data and information views for operational and analytical purposes.

Figure 5-4 – Unified OCW Model

This should be accomplished in an iterative process, managed under a strategic program similar to the framework illustrated below.
5.2.1 **RECOMMENDED STEPS TO IMPLEMENT MDM**

1. **The Data Governance Framework should be established before starting MDM.**

   MDM is a specialized subset of data governance and data management. Establishing data governance and data management first lays the foundation for MDM to build upon. The roles, processes, and technology needed to support MDM can be layered on top of data governance and data management.

2. **The business need for MDM, in addition to data management, needs to be justified.**

   MDM involves creating a unified view of similar data that comes from disparate sources, many of which may be outside of OCW control. The business case for MDM, in the context of ROA and data analytics, needs to be justified.

3. **MDM readiness should be assessed.**

   The data quality of all target data sources should be evaluated to determine the level of effort needed to create a single view of a given master data subject area. Based on the
evaluation, the best approach should be determined to incrementally add data sources to a data subject area selected for MDM.

4. **The MDM Framework should be defined and documented, clearly defining its objective and purpose.**

   The goal of this recommendation is the same as defining the Data Governance Framework, expect the initiatives specific to MDM should be considered. Once a MDM subject area is chosen, consider the unique aspects of creating a master data reference file for that subject. Efforts should be coordinated with the agencies involved to ensure a common understanding of what the data means (i.e., agree on a common data dictionary and common metadata for the data elements involved). The risks and challenges in creating the master data view should also be clearly understood and documented.

5. **Policies and procedures should be documented, clearly describing the planned operational aspects of MDM.**

   The goal is to accomplish the same items recommended under data governance and data management, including the additional MDM specific needs, which primarily consist of identifying the System of Record (SOR) for each master data domain. The SOR is the most reliable source for a given data element or piece of information. Since information in a master data domain may come from many different data sources, it is important to know the authoritative source for each data element.

6. **MDM Technical Architecture and Tools should be established.**

   This also builds upon what is defined for data management to support the unique needs of MDM. The master data model should be defined, as well as any ancillary data that can be linked to the master data domain. Algorithms should be developed that define how the data from disparate data sources will be matched to create the master view. Threshold rankings should be defined to determine what can be automatically matched or dismissed versus what matches will need human intervention. The data cleanup, conversion, and standardization approach should be defined, as well as the data stewards responsible for the work.

7. **A Proof of Concept (PoC) should be conducted.**

   A PoC should be defined and executed under a small-scale highly controlled scenario to validate the MDM processes developed. The parameters of the PoC should allow for easy and obvious identification of problems to make MDM process revision as quick as possible.
5.3 DATA SHARING AND DATA ACQUISITION

North Highland recommends that DCF/OCW plan its work to reach Level 2 maturity in improving their capability to share and acquire data for operations and insight as its next step, as indicated by the figure below.

Drivers
- Valuing data as an insightful asset
- State legislators want to share data
- Agencies want to share data
- Lawyers are instructed to find ways to share

Facilitators
- Adhering to data exchange standards
- Service Oriented Architecture (SOA)
- Enterprise Service Bus (ESB)
- Development “accelerator” packages

Figure 5-6 – Data Sharing Maturity Model

5.3.1 RECOMMENDED STEPS TO IMPLEMENT DATA SHARING AND DATA ACQUISITION

1. The business need to share data should be identified.

Everyone involved in the data sharing initiative should understand the reason OCW is requesting the data and should agree that the reason is justified.

2. The metadata for the data elements involved needs to be documented.

It is common for the word “client” to mean different things to different agencies. Everyone involved should agree as to what the data elements being requested represent to ensure the data being requested will satisfy the business needs. The characteristics of each data element should be documented. The data elements should then be grouped into common subject areas (data categorization). This may help identify the best source for each data group.
3. **The most reliable source for each data subject area should be identified.**

   Building on the SOR concept described for MDM, the best source to acquire data elements for each subject area should be identified. For instance, if the data subject area is Provider, the group responsible for Provider Data Management may be the best source to obtain reliable Provider data.

4. **Obstacles to sharing data should be identified and mitigated as early as possible.**

   It is important to understand any legal limitations or security barriers early. Attempts to identify ways to overcome the barriers are needed, but if that is not possible, other sources for the data needed should be identified.

5. **Good communication is a key element to success.**

   The appropriate communication channels should be developed to ensure data being requested and the consequences of sharing the data are known by the relevant people.

6. **The Data Sharing Agreement (DSA) should contain the appropriate content.**

   The DSA is a legal document that should be complete enough to cover all anticipated circumstances. It should include the items needed to cover any circumstances regarding the data, as well as sharing and exchanging the data. A complete list of suggested content is included in the Data Sharing and Data Acquisition Checklist in Appendix 6.

7. **Data acquisition should be automated.**

   Once the DSA is approved, data stewards and technicians should work together to define automated processes for data exchange, with the goal of making the processes as repeatable and consistent as possible. Data profiling and data quality processes should be developed to ensure the data files comply with the metadata. The technology infrastructure on each side of the exchange needs to be compatible and must enforce security requirements.
SECTION 6  FUTURE STATE IN FLORIDA

6.1  FUNCTIONAL ORGANIZATION AND GOVERNANCE REQUIRED TO SUPPORT FUTURE STATE

The Data Governance Framework enables managing the OCW data environment and maintaining data quality. The organization will foster excellence through formal practices, standards, and measures that ensure compliance to documented governance processes and procedures. The Data Governance Framework will centralize enterprise-wide access to data to eliminate duplicate databases, comply with security and privacy legislation, and to promote a central, authoritative source of information. Through this organization, efficiency in OCW’s systems will increase to align with OCW’s goals to improve the deployment of analytics related to child safety and ROA mandates.

Figure 6-1 – Data Governance Framework Vision

6.1.1  GOALS AND OBJECTIVES

The objectives of the Customer Data Governance Framework are to:

- Align state and agency objectives and initiatives involving enterprise data.
- Establish and maintain formal data governance practices, standards and measures for data usage, data sourcing, data hygiene, data quality, data archiving and agency rules.
Establish and maintain formal processes and procedures to ensure compliance to governance practices, standards, and measures.

Establish roles and responsibilities for the management and ownership of subject area data.

Ensure compliance to customer data security and privacy legislation.

Communicate data governance issues to appropriate OCW end-users and agency units.

Drive and improve efficiency in systems and processes in their use of subject area data.

Establish a common taxonomy and terminology.

Establish data advocacy and ensure data is treated as a valuable agency asset.

6.1.2 ORGANIZATIONAL HIERARCHY

The figure below illustrates the key interactions of roles within the agency data governance model. Roles are grouped into two main layers (i.e., leadership and stewardship) and promote the communication between agency, IT, and project teams.
6.2 DATA SHARING AGREEMENTS AND DATA ACQUISITION

A Data Sharing Agreement (DSA) should supplement and not supplant an overall data management plan. However, if both are completed, they will share several elements. Developing a DSA is about relationship building, trust building, good communication, compromise, long-term planning and finding ways to openly and safely share to maximize the use of the hard-earned data and information. It is about determining legally and ethically appropriate ways to disseminate the data to improve data quality and integrity for all parties involved. The technical aspects of data acquisition need to be determined for each data exchange project, but the processes must be monitored under established data governance and MDM policies and procedures.
Appendix 6 lists the steps necessary to accomplish data sharing and data acquisition. It also includes the Data Acquisition Playbook, providing more insight into how the steps are performed. The Data Acquisition Playbook is presented in a process flow and tabular format.
SECTION 7 GAPS

7.1 DATA GOVERNANCE AND DATA MANAGEMENT

DCF and the state of Florida see the need for formal data governance, but there is currently no formal committee or documented processes. Recent Florida legislative bills (SB 1430 and HB 1195) were proposed to create the position of Chief Data Officer (CDO), which required the CDO to perform many of the functions described here for data governance and data management. However, the bills failed to pass.

There is a workgroup within DCF for those using Tableau, but it is meant to address technical concerns and therefore it is tactical rather than strategic. The workgroup has just started and has only met a few times. There currently is no documentation to build upon in establishing data governance or data management processes.

DCF believes there are processes in place to share data internally among the three DCF Programs (OCW, SAMH, and ESS), but the existing processes only account for operational needs, not data analytics. These operational processes are not formally documented to allow for re-use and repeatable execution.

DCF sees a need to build a business-friendly data dictionary and metadata repository for its databases. IBM does maintain a technical data dictionary, but it is not easy for the business community to use. DCF would like to establish the documented meaning behind all of its data elements so that everyone has a common understanding of what the data means. This would also support data cleansing and data quality initiatives it would like to undertake. OCW stated that it would like to address this by working closely with DCF and the Tableau workgroup to:

- Establish a Data Governance Committee for leadership and strategic direction,
- Develop standard processes and best practices for data management especially in support of data analytics.

7.2 MASTER DATA MANAGEMENT

There is a DCF initiative underway to build a “Client ID” table that will link clients across three programs. This is driven out of the DCF Secretary’s office and is led by the DCF Procurement Manager. This effort has just started and is in an exploratory phase. There currently are not many formal processes and standards established. The “Child Golden Record” proposed in the document is a subset of the clients. This would be an opportune moment for OCW to collaborate on this effort and for DCF, as a whole, to consider the recommendations made in this document.

DCF sees a need to improve the IT infrastructure and tools used to support data quality and master data management (MDM). DCF also sees the need to improve data quality within its systems before addressing data quality across systems.
7.3 DATA SHARING AGREEMENTS AND DATA ACQUISITION

Currently, much more data is being exported from DCF to other agencies that is being imported into DCF from other agencies. OCW would like to receive data from several other agencies to support its long term ROA and data analytics goals. There are some Data Sharing Agreements (DSAs) currently in place, but they provide access to a small subset of the data needed.

OCW sees the current process to get a DSA in place as unnecessarily slow. For example, the initial meeting to discuss data sharing with SAMH was requested on 1/12/2016. After several meetings and revisions to the DSA, it was executed on 3/30/2016. While there is a basic template DCF uses, the process generally starts from the beginning every time. There are no standards or processes agreed upon across agencies to make the boilerplate repetitive tasks quick and easy. There is also the perception that requests are made for all the data elements and all the data records in a data file as opposed to requesting clearly defined specific data to satisfy a specific business need.

Once a DSA is approved, the process of acquiring the data is also laborious. There are few, if any, standard data exchange formats or methods. The formats and methods used require significant manual intervention, and there are few automated notification, data profiling, or exception handling processes that support receiving data from external sources.

OCW stated that they would like to address this by:

- Increasing the use of automated, repeatable processes in receiving external data,
- Decreasing the multiple duplicate versions of data that currently exists (have a “single version of the truth”), and
- Improving the data “timeliness”, ensuring the data being used is as current as needed.
SECTION 8 IMPLEMENTATION ROADMAP

8.1 OVERVIEW

The multi-year roadmap is a high-level plan highlighting major activities, estimated durations, dependencies, and expectations for the macro plans related to the three major critical initiatives – data governance, master data management, and data acquisition and sharing. The roadmap is supported by abstracts detailing key benefits, stakeholders, resource requirements, milestones, potential challenges, critical success factors, and budget impact.

8.2 THE BUSINESS CASE FOR CHANGE

The long-term assurance of child welfare is DCF/OCW’s number one goal and is only achieved when a consolidated view of relevant information from all key data sources (e.g., FSFN, DJJ, Mental Health, ACCESS) is available to caseworkers and front line analysts in a timely fashion.

- The true value of data governance and master data management processes is only realized when they extend outside of OCW.
- The application of key data management processes like entity resolution and data cleansing of FSFN data is tactically relevant and is a piece of the overall value, but does not constitute data governance or master data management.
- Piloting comprehensive data governance and master data management best practices with key OCW-controlled data sources accelerates adoption, models a sustainable foundation that can be extended at DCF, and becomes an accelerator in gaining support for the broader cross-agency business case.

8.3 INITIATIVES, TIMELINES, AND TASKS

This section includes individual initiative overviews listing goals, key tasks, risks, success factors, anticipated resources, and budget impact. It also contains a roadmap of the high-level tasks for implementation and operation of data governance, data management, master data management, and data sharing. Further breakdown of the tasks will be required as the projects are initiated. The Gantt charts may be used as a guide to the sequencing of the tasks over the timeframe described. A more detailed listing of the timeline tasks and sequencing dependencies is also included.

All estimates are rough order of magnitude for planning purposes. Dates and other attributes of the estimates may change as scope is refined prior to project initiation. It is important to consider that there are already a number of existing initiatives that require OCW and DCF resources; therefore, funding and resources to support these new initiatives must be prioritized along with existing initiatives.
8.3.1 **Data Governance Initiative**

The graphic below gives an overview of the Data Governance Initiative, listing goals, key tasks, risks, success factors, anticipated resources, and budget impact.

![Data Governance Initiative](image)

**Figure 8-1 – Data Governance Initiative**

8.3.2 **Data Governance Timeline**

The following Gantt chart may be used as a guide to the scheduling of initial and on-going iterative initiatives. Timelines are approximate and should be reevaluated as needed based on resource capacity to support parallel processes. References to data management includes master data management.
Figure 8-2 – Data Governance Tasks and Timeline
8.3.3 DATA GOVERNANCE TASK DESCRIPTIONS

More descriptive information about the tasks in the data governance timeline above is provided below.

1. Establish Communication Strategy and Change Management Strategy

   The communication strategy builds support for data as a valuable asset, within an agency and across agencies. It will facilitate the approval of all the planning documents and processes supporting data governance including the business case and the charter. Execution of the communication strategy will be continued throughout all the tasks described in the timeline above.

   The change management strategy will describe the plan to implement the organizational changes needed to enact data governance and data management. Execution of the change management strategy takes place in the late stages of planning and throughout implementation and operations.

2. Establish Data Governance (DG) Business Case

   The business case will show that the benefits of data governance outweigh the costs. It will also identify the funding strategy and sources to sustain the program. The data governance objectives described in the business case need to align with Agency and State goals and objectives, including:

   a) Person ID work led by the DCF Procurement Manager at the DCF level
   b) DCF Operational Performance (OP) work led by the DCF Planning Director
   c) Analytics that is part of the DCF OP work
   d) The child-focused work led by the governor’s office

3. Establish DG/Data Management (DM) Framework and Charter

   This task has a dependency on another task in the timeline: Establish Data Governance (DG) Business Case – Start Establish DG/Data Management (DM) Framework and Charter after the Data Governance Business Case is approved.

   The Framework and Charter will give everyone a common understanding of the data governance purpose and structure by:

   a) Defining the Data Governance Objectives
   b) Defining Guiding Principles
   c) Defining Roles and Responsibilities
   d) Identifying the metrics and KPIs to measure success
4. Designate DG Decision Making Bodies

**This task has a dependency on another task in the timeline:** Establish Data Governance (DG) Business Case – Start Designate DG Decision Making Bodies after the Data Governance Business Case is approved.

The Executive Steering Committee and the Data Governance Board need to be established. The Executive Steering Committee will set strategy and provide guidance and oversight. The Data Governance Board will provide the direction to execute strategy and to manage data-to-day operations.

5. Document DG/DM Policy and Procedure

**This task has a dependency on two other tasks in the timeline**


II. Designate DG Decision Making Bodies – Document DG/DM Policy and Procedure cannot finish until after the Decision Making Bodies are in place to approve policies and procedures.

Effective data management is realized by defining policies and procedures that ensure data quality, integrity, and security. The roles, responsibilities and decision rights of human resources that manage, execute, and monitor the policies and procedures must also be defined.

6. Establish DM Architecture and Processes

**This task has a dependency on another task in the timeline:** Document DG/DM Policy and Procedure – Establish DM Architecture and Processes cannot finish until after Document DG/DM Policy and Procedure is complete and the architecture and process requirements are final.

The data management architecture and processes, from both the business and the IT perspective, will be designed. People, processes, and technology must be considered in this step. Also, the entire Data Life Cycle must be taken into account, from intake until it is no longer used.

7. Identify Supporting DM Infrastructure and Tools

**This task has a dependency on another task in the timeline:** Establish DM Architecture and Processes – Identify Supporting DM Infrastructure and Tools cannot finish until after Establish DM Architecture and Processes is complete and the supporting infrastructure and tools requirements are final.
Once the data management requirements are known, the supporting infrastructure and tools can be identified. The requirements need to cover topics such as:

a) Data access, retrieval and life cycle management  
b) Data modeling and metadata management  
c) Data quality, data profiling, and business rules validation  
d) Storage and security  
e) Data remediation and exception handling  
f) Automation, re-use and repeatable processes

8. Implement and Execute DG/DM

This task has a dependency on two other tasks in the timeline

I. Identify Supporting DM Infrastructure and Tools – Start Implement and Execute DG/DM after identification of supporting infrastructure and tools is complete.

II. Evaluate USF PSRDC Capability to Support OCW Objectives – Start Implement and Execute DG/DM after evaluation of USF’s capability to support OCW objectives is finalized.

At this point OCW should be ready to put the plans in action by implementing and executing data governance and data management. In doing so, it is important to account for the people, processes, and technology that must be in place to accomplish the goals.

a) The roles defined during planning must be filled to support design, development, and operations.  
b) The operational use cases and business process flows must be documented and automation requirements must be defined.  
c) Data models and software applications to support automation must be designed, developed, and implemented.  
d) Once data governance and data management are operational, procedures to manage issues, maintenance, and enhancement requests must be established.

9. Continuously Monitor, Measure and Revise DG/DM

This task has a dependency on another task in the timeline: Implement and Execute DG/DM – Start Continuously Monitor, Measure, and Revise DG/DM after the Implement and Execute DG/DM initial implementation work is complete.
Once processes are implemented, they must be monitored for areas of improvement and revision. Key Performance Indicators (KPIs) and metrics must be monitored to ensure the program is accomplishing the expected results and goals.

10. Evaluate USF PSRDC Capability to Support OCW Data Governance/Data Management Objectives

This task has a dependency on two other tasks in the Timeline

I. Establish DG/Data Management (DM) Framework and Charter – Start Evaluate USF PSRDC Capability to Support OCW Objectives after the Data Governance Charter is approved and the program objectives are final.

II. Identify Supporting DM Infrastructure and Tools – Evaluation of USF PSRDC’s capability to support OCW objectives cannot finish until after supporting infrastructure and tools requirements are final.

There is a risk associated with this task: OCW may decide to start implementing some Proof of Concept (PoC) projects at USF PSRDC before processes are finalized and the architecture, infrastructure, and tools to support OCW objectives are finalized. This may result in deliverables that are not usable or need significant re-work after the Document Policy and Procedure, Establish Data Management Architecture and Processes, and Identify Supporting Infrastructure and Tools initiatives are complete.

As part of evaluating USF PSRDC capability, OCW must consider a number of factors, including:

a) The ability of the infrastructure, tools, and technology to support OCW data governance and data management objectives.
b) The ability to support OCW data governance and data management objectives regarding metadata and data dictionary maintenance processes.
c) The ability to support OCW data governance and data management objectives regarding data quality and business process flows.
d) The ability to monitor and report OCW data governance and data management objectives regarding metrics and KPIs.
e) The data life cycle management capability to support OCW data governance and data management objectives.
8.3.4 **MASTER DATA MANAGEMENT INITIATIVE**

The graphic below gives an overview of the Master Data Management Initiative, listing goals, key tasks, risks, success factors, anticipated resources, and budget impact.

![Figure 8-3 – Master Data Management Initiative](image)

8.3.5 **MASTER DATA MANAGEMENT TIMELINE**

The following Gantt chart may be used as a guide to the scheduling of initial and on-going iterative initiatives. Timelines are approximate and should be reevaluated as needed based on resource capacity to support parallel processes.
Figure 8-4 – Master Data Management Tasks and Timeline
8.3.6 Master Data Management Task Descriptions

More descriptive information about the tasks in the Master Data Management Timeline above is provided below.

1. Integrate MDM with DG/DM Strategy and Planning Initiatives

   Include MDM in the data governance and data management planning effort for the business case and the charter.

2. Evaluate and Select MDM Tools and Architecture

   This task has a dependency on another task in the timeline: Planning and business case activities with DG/DM – Start Evaluate and Select MDM Tools and Architecture after the DG/DM planning and business case activities are complete.

   Once the MDM requirements are known, the supporting infrastructure and tools can be identified. The requirements need to cover topics such as:

   a) Creating a single view of the data
   b) Associating related data to create the 360-degree view of a master data domain
   c) Sharing master data across the enterprise

   These tools are in addition to the data management tools that support data profiling, data cleansing, etc.

3. Implement Selected MDM Tools and Architecture

   This task has a dependency on another task in the timeline: Evaluate and Select MDM Tools and Architecture Data Management – Start Implement Selected MDM Tools and Architecture after Evaluate and Select MDM Tools and Architecture is complete.

   At this point, OCW is ready to implement the tools and processes unique to MDM, on top of the data management implementation. It is important to take into account:

   a) How the human resource roles are changed or augmented to support MDM.
   b) The operational use cases and business process flows unique to MDM must be documented and automation requirements must be defined.
   c) Data models supporting the master data domains and software applications to support automation must be designed, developed, and implemented.
   d) Once operational, procedures to manage issues, maintenance, and enhancement requests unique to MDM must be established.
4. Reconcile Corollary Efforts and Define Person Golden Record (PGR)

This task has a dependency on another task in the timeline: Planning and business case activities with DG/DM – Start Reconcile Corollary Efforts and Define Person Golden Record (PGR) after the DG/DM planning and business case activities are complete.

The child subset of the PGR will provide the central master data domain to which other data related to the child’s welfare will be associated. OCW can collaborate with DCF on the Client Data Link project already underway. DCF has started a project to match people across the all systems the agency uses, essentially creating a Master Client Index (MCI). Additionally, OCW can use the MCI to establish relationships between a child and the other people influencing the child’s welfare.

5. Implement PGR in MDM Framework

This task has a dependency on two other tasks in the timeline

I. Implement Selected MDM Tools and Architecture – Start Implement PGR in MDM Framework after Implement Selected MDM Tools and Architecture is complete.

II. Reconcile Corollary Efforts and Define Person Golden Record (PGR) – Start Implement PGR in MDM Framework after Reconcile Corollary Efforts and Define Person Golden Record (PGR) is complete.

The first step in creating the holistic view of the child is to implement the data model and processes required to build the PGR, including a child attribute to identify the children within the PGR. All PGR data conversion, cleanup, and integration need to be thoroughly tested and revised to ensure the expected results are achieved.

6. Execute and Evaluate a Pilot Analytics Project Using the PGR

This task has a dependency on another task in the timeline: Implement PGR in MDM Framework – Start Execute and Evaluate a Pilot Analytics Project Using the PGR after Implement PGR in MDM Framework is complete.

A pilot project should be defined and executed under a small-scale highly controlled scenario to validate PGR functionality. The parameters of the pilot project should allow for easy and obvious identification of problems to make process revisions as quick as possible.

7. Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV)
This task has a dependency on another task in the timeline: Implement PGR in MDM Framework – Start Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV) after Implement PGR in MDM Framework has started.

Once the PGR business rules and automated processes are stable, relationships can be added to the child subset within the PGR, creating the Comprehensive Child View (CCV) hub. People and events related to child welfare can be associated to the CCV hub forming a 360-degree view of the child’s ecosystem. The CCV will show relationships of people that constitute the child’s family and household environment. Health and judicial information for the child and related people can all be associated to the child. The CCV model will be the basis of future Data Analytics and research supporting ROA.

8. Expand Cross Functional Use of CCV

This task has a dependency on two other tasks in the Timeline

I. Execute and Evaluate a Pilot Analytics Project Using the PGR – Start Expand Cross Functional Use of CCV after Execute and Evaluate a Pilot Analytics Project Using the PGR is complete.

II. Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV) – Start Expand Cross Functional Use of CCV after Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV) is complete.

Ideally, the CCV should mature beyond OCW and DCF use alone. The long-term vision is for all state agencies affecting child welfare to use CCV and share data to build a “single view of the truth” concerning the child. This starts by communicating with key agencies to publicize the CCV and its benefits. DCF should collaborate with the agencies to design processes and a roadmap that will add their child-related data to the CCV.

9. Automate Overall Data Quality, and Integrity Processes for CCV

This task has a dependency on another task in the timeline: Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV) – Start Automate Overall Data Quality, and Integrity Processes for CCV after Enrich PGR Child Subset with Additional Data to Create the Comprehensive Child View (CCV) has started.

Once the benefits of the CCV are realized, continue adding data from other agencies. The CCV should be shared across agencies, becoming the state’s System of Record for data related to child welfare.
10. Evaluate USF PSRDC Master Data Management Technical Capabilities

This task has a dependency on another task in the Timeline: Evaluate and Select MDM Tools and Architecture – Start Evaluate USF Master Data Management Technical Capabilities after the MDM tool requirements are defined.

Once the MDM tool requirements are known, the tools being used at USF PSRDC can be evaluated to determine how well they meet OCW’s needs.
**8.3.7 DATA SHARING AND DATA ACQUISITION INITIATIVE**

The graphic below gives an overview of the Data Sharing and Data Acquisition Initiative, listing goals, key tasks, risks, success factors, anticipated resources, and budget impact.

- **Project Goals**
  - Remove barriers to sharing the data needed to accomplish OCW business objective and goals
  - Establish a collaborative statewide child welfare community
  - Improve the management, quality, and integrity of state data sources
  - A holistic view of child welfare information (Comprehensive Child View (CCV))
  - Full participation by all stakeholders

- **Stakeholders**
  - **Internal:**
    - OCW executive leadership and management
    - OCW staff
  - **External:**
    - Other DCF department leadership
    - DCF leadership
    - CBCs
    - Other FL agency data sources

- **Key Tasks**
  - Define and understand the data needed
  - Identify the best data sources
  - Justify the need to acquire data
  - Communicate with DSOs early to build trust and cooperation
  - Develop a DSA template and a step-by-step repeatable process (playbook) that expedites approval
  - Establish standard data exchange protocols
  - Expand support for a common data sharing framework starting with key agencies and leading to the state level

- **Risks/Challenges**
  - Cross-agency executive support
  - Data sharing obstacles (legal, security, etc.)
  - Data quality and integrity
  - Coordinating and communicating metadata changes

- **Success Factors**
  - A complete view of all factors affecting a child’s welfare
  - Intra and inter-agency sharing of data and child welfare case management

- **Milestones**
  - TBD

- **Team/Resources**
  - **Executive Sponsor(s):**
    - Secretary, DCF
    - Asst. Secretary, OCW
    - OCW Perf & Quality Mgmt Director
    - OCW C/O
  - **Project Management and Resources:**
    - OCW/North Highland
  - **Subject Matter Experts:**
    - OCW
    - CBC
    - North Highland/SAS
    - USF

- **Budget Impact**
  - Additional internal resources
  - Potential funding, coordination with data source organizations

**Figure 8-5 – Data Sharing and Data Acquisition Initiative**

**8.3.8 DATA SHARING AND DATA ACQUISITION TIMELINE**

The following Gantt chart may be used as a guide to the scheduling of initial and on-going iterative initiatives. Timelines are approximate and should be reevaluated as needed based on resource capacity to support parallel processes.
Figure 8-6 – Data Sharing and Data Acquisition Tasks and Timeline
8.3.9 DATA SHARING AND DATA ACQUISITION TASK DESCRIPTIONS

More descriptive information about the tasks in the Data Sharing and Data Acquisition Timeline above is provided below.

1. Integrate Data Acquisition with Data Governance/Data Management Strategy and Planning Initiatives

   Include data sharing and data acquisition in the data governance and data management planning effort for the business case and the charter.

2. Identify the Data Needs

   This task has a dependency on another task in the timeline: Integrate Data Acquisition with Data Governance/Data Management Strategy and Planning Initiatives – Start Identify the Data Needs after the Data Governance Charter is approved and the program objectives are final.

   The specific data elements needed to meet the ROA and data analytics business objectives need to be identified.

3. Document the Metadata

   This task has a dependency on another task in the timeline: Identify the Data Needs – Document the Metadata cannot finish until after the identification of all data needs is final.

   The goal of this task is to document the meaning and data characteristics of each data element to ensure a common understanding across departments or agencies involved in sharing the data. Additionally, categorizing the data into related subject areas will help OCW identify the best source for each data category and reduce redundant data requests from multiple external sources.

4. Identify the Data Sources

   This task has a dependency on another task in the timeline: Document the Metadata – Identify the Data Sources cannot finish until after the metadata documentation is final.

   Once the Metadata is documented, OCW can determine the best source to acquire each data category.

   a. Data Categories available through FSFN
   b. Data Categories available through other OCW systems
   c. Data Categories available through other DCF departments
d. Data Categories required from external sources

5. Develop a DSA template

This task has a dependency on another task in the timeline: Integrate Data Acquisition with Data Governance/Data Management Strategy and Planning Initiatives – Start Develop a DSA template after the Data Governance Charter is approved and the program objectives are final.

The DSA should be complete enough to cover all anticipated circumstances. It should include the items needed to cover any circumstances regarding the data, as well as sharing and exchanging the data. A complete list of suggested content is included in the Data Sharing and Data Acquisition Checklist in Appendix 6.

6. Establish DSAs with Data Sharing Organizations

This task has a dependency on two other tasks in the timeline

I. Develop a DSA template – Start Establish DSAs with Data Sharing Organizations after the DSA template is final.

II. Evaluate USF PSRDC Capability to Support OCW DA Objectives – Initial work for Establish DSAs with Data Sharing Organizations should not finish until after the initial work on Evaluate USF PSRDC Capability to Support OCW Data Acquisition Objectives is final.

Appendix 6 of this document includes a checklist and process flows to establish a DSA with an external data source.

7. Data Acquisition

This task has a dependency on another task in the timeline: Establish DSAs with Data Sharing Organizations – Start Data Acquisition with a specific data sharing organization after the DSA is final.

Appendix 6 of this document includes a checklist and process flows to acquire data from an external data source once the DSA is finalized.

8. Continuously Monitor, Measure and Revise Data Acquisition

This task has a dependency on another task in the Timeline: Data Acquisition – Start Continuously Monitor, Measure, and Revise Data Acquisition after the Data Acquisition initial implementation work is complete.
Once data acquisition processes are implemented, they must be monitored for areas of improvement and revision. There may be federal or state legislative changes that require DSA changes or changes to the ways data is exchanged. Changes in the data characteristics may require changes to the data exchange processes and supporting metadata.

9. Expand Support for a Common Data Sharing Framework

This task has a dependency on another task in the Timeline: Continuously Monitor, Measure and Revise Data Acquisition – Start Expand Support for a Common Data Sharing Framework after the initial “lessons learned” and revisions are made to establishing DSAs and acquiring data.

Once a stable DSA is formulated, communicate with other key agencies to build support for the use of a common DSA template. OCW and DCF can work with state level organizations to address data sharing legal barriers and to elevate support for data governance, MDM, and data sharing to the state level.

10. Evaluate USF PSRDC Capability to Support OCW Data Acquisition Objectives

This task has a dependency on three other tasks in the Timeline

I. Identify the Data Needs – Start Evaluate USF PSRDC Capability to Support OCW Data Acquisition Objectives after the initial Identify the Data Needs work is complete.

II. Document the Metadata – Start Evaluate USF PSRDC Capability to Support OCW Data Acquisition Objectives after the initial Document the Metadata work is complete.

III. Identify the Data Sources – Start Evaluate USF PSRDC Capability to Support OCW Data Acquisition Objectives after the initial Identify the Data Sources work is complete.

Once the identified dependencies are satisfied, OCW can evaluate the USF PSRDC capability to support OCW Data Acquisition objectives by taking the following steps:

a. Identify the Data Categories available at USF PSRDC
b. Determine if the Data Categories not available can be added as USF PSRDC
c. Determine if sufficient Data Categories can be made available to meet the OCW business objectives
d. Determine if all the stakeholders needing data access can get it
e. Consider the consequences of USF PSRDC being the data repository
   i. Coordination with data requirements and data storage for data analytics needs
ii. Clearly defined roles and responsibilities between USF PSRDC, data analytics delivery partner, and OCW personnel
SECTION 9 CONCLUSION

Proper data governance, MDM, and data acquisition strategy, organization, processes, and infrastructure are key ingredients to OCW realizing its goals for the ROA and data analytics initiatives. Proper planning before execution is critical to making the data governance and management strategies succeed.

The main objective of this document is to:

- Describe a data governance framework to support better communication between agencies and facilitate cross-agency data sharing
- Describe best practices and procedures for data management and MDM
- Present a step-by-step repeatable process to identify and acquire data needed from external sources
- Propose the organizational structure best suited to support the objective listed above.

North Highland believes that following the recommendations presented in this document will help OCW achieve its desired future state. Implementing the recommendations based on the initiatives, timelines, and tasks described in this document will allow for the proper planning and sequencing of projects required to successfully satisfy the initiatives.
SECTION 10 APPENDICES

10.1 APPENDIX 1 – MEETING NOTES FROM CURRENT STATE MEETINGS

10.1.1 FIRST MEETING

The first meeting held included the Manager of Performance Management, the Director of Performance and Quality Management and the Child Welfare Performance Management Analyst from OCW. The purpose of the meeting was a Data Assessment Walkthrough for the Florida Safe Families Network (FSFN) and the DCF Date Warehouse (DW), but some things relevant to data governance, MDM and DSAs were discussed.

It was stated that OCW should know more about its own data (e.g., FSFN) before receiving and evaluating data from external sources. The focus should be on what OCW wants to know (the Research Questions) when assessing the data, starting with a focus on reducing re-maltreatment. A FSFN Adoption project is underway to re-educate the Community-Based Care agencies (CBCs) on FSFN capabilities and encourage them to use FSFN as the system of record for all OCW related work. A consequence of the primary goal would be improved data quality and content in FSFN.

10.1.2 SECOND MEETING

Another meeting was held with the Manager of Performance Management to get an understanding of how the Performance Management department operates. Performance Management is the production-focused aspect of providing information to support processes such as federal reporting and compliance, day-to-day operations and executive reporting needs.

The OCW Performance Reporting Manager uses the DCF DW to create some data marts and Excel pivot tables used to produce the Spinner Reports. The Spinner Reports are child protective investigative trend reports that provide access to investigation related data trends on a state, region, or circuit level. The reports are posted to a public-facing website (Florida’s Center for Child Welfare) hosted by the University of South Florida (USF). A data visualization product named Tableau is used to produce OCW reports based on the data repositories the Reporting Manager’s group creates and the DCF DW. There is a committee supporting Tableau and the associated data, but it is not a data governance committee per se.

Regarding DSAs, the Performance Management Department Manager has executed some data DSAs and there are existing templates. An additional DSA was finalized in March 2016 to get data from Florida Healthy Families. DSAs are also needed to get data from and Florida Department of Juvenile Justice (DJJ) and the Florida Department of Health (DOH).
10.1.3 Third Meeting

The next meeting was held with the DCF Chief Information Officer (CIO) and the Director of Performance and Quality Management. The purpose of the meeting was to identify any current DCF standards and/or processes supporting:

1. Data governance
2. MDM
3. Data Acquisition/Data Sharing

The DCF CIO explained that there is no specific IT activity around data governance. He stated there was an effort to link data across agencies in the past, but the legislative and regulatory restrictions caused so many problems that the project was shut down. He added FSFN and the Economic Self-Sufficiency System (ACCESS) are linked but there is no Master Patient Index (MPI) across agencies. In separate meetings, the DCF CIO and the DCF Procurement Manager said DCF has an MPI, but it is not currently used for much. It was also pointed out that eligibility data supporting social service programs and Medicaid is currently integrated at the Agency for Health Care Administration (AHCA), but the programs are not sharing medical claims or encounters data.

Most data exchanged is going outward from ACCESS, not much from FSFN. Each request is handled on a point-to-point case-by-case basis. Each DSA requires legislative review. Once the DSA is approved and signed, the actual exchange of data is handled through a point-to-point Secure File Transfer Protocol (SFTP) connection. There are no formal processes or specific resources dedicated to MDM or data sharing.

Any technical work required from DCF to support OCW data exchange is prioritized along with all other OCW IT support from DCF. The hours, and funding, required to support the effort are allocated from the overall “pool” of hours and funding allocated to OCW for a given fiscal year. The Director of Performance and Quality Management pointed out that the data currently exchanged to support OCW is managed by the Performance Management Department Manager and does not involve DCF’s IT organization.

Going forward, the DCF CIO would like to be involved in the DCF/MDM/Data Sharing process. He believes he has resources that can support the effort. The DCF CIO would like to see the data governance process extend to the operational world. He believes the process should be built around priorities rather than programs. He believes he can guide OCW down the right path if OCW works with him along the way. The Director of Performance and Quality Management will work with the DCF CIO to explain what is being done with ROA and data analytics and determine where they can work together.

10.1.4 Fourth Meeting

The next meeting was held with the Director of Performance and Quality Management and the Performance Management Department Manager. The purpose of the meeting was to identify any current OCW standards and/or processes supporting:
1. Data governance
2. MDM
3. Data Acquisition/Data Sharing

The Performance Management Department Manager pointed out that any data stores his group creates are to support reporting. It is a much smaller scale than the DCF DW. There is no formal structure supporting data governance or MDM at OCW. There are no formal processes that OCW adheres to other than what is described in each DSA. Actual adherence to the DSA is handled on a trust basis, not on an audit basis; OCW is not staffed for that. The Performance Management group has created some sets of code particular to the needs of each DSA, but the code is not set up to process automatically. Minor configuration changes are needed as each data set is retrieved and the code is executed manually through completion. OCW is in the process of setting up an automated data exchange with AHCA now.

The OCW agency SMEs work directly with the Performance Management Department Manager to define the data needed and he takes it from there, developing and executing the DSAs. DSAs are negotiated on a case-by-case basis, starting with an OCW template. The Point of Contact may be different for each DSA. Small data transfers are handled through encrypted email. Larger files are done through SFTP. Data intake is done by linking directly to the data source provided (e.g., an Excel file).

There is no formal data transmittal or receipt acknowledgement process. None of the data OCW currently exchanges are supported by “generic” processes (e.g., web services). Everything is done on a case-by-case, point-to-point process. Since there are no formal processes, there is no documentation other than the DSAs. Files are received in various formats, including, but not limited to:

- Excel files
- ASCII flat files
- Delimited Unicode flat files

The format of the file is determined as the DSA is being negotiated.

CFOP 50-26, Policy on Agreements Involving Data Sharing, describes the DCF operating procedures and guidelines to set up and execute a DSA. OCW is currently exchanging data with DJJ and the Florida Agency for Persons with Disabilities (APD). For APD, OCW sends a data file, and then APD performs data matching processes against APD data and sends a file back.

---

7 URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjTt9m8wPPMAhXDbB4KHV29D3wQFggdMAA&url=https%3A%2F%2Fwww.dcf.state.fl.us%2Fadmin%2Fpublications%2Fcfops%2Fcfop%2520050-26%2520Systems%2520Management%2520Agreements%2520Involving%2520Data%2520Sharing.pdf&usg=AFAQjCNHRq6KZvrt_UL5Oz5wcmJBhC9dVtw
10.1.5 Fifth Meeting

The last interview was a phone call with the DCF Procurement Manager. This contact was initiated as a result of information the Manager of Performance Management provided regarding a data user group associated with Tableau. The Procurement Manager explained that, while the group does discuss data sharing, they do so from the technical aspect of the methods to get and store the data, not the procedures required to establish DSAs. He pointed out that this is a new group that has only met twice, so there is not any current documented results or outcomes.

His description of the DSA process agreed with what was said by others. It is a lengthy process that is negotiated on a case-by-case basis involving agency work groups and legal counsel. Each agency has its own process and sometimes its own DSA. If the agency’s process is not followed, data will not be received from that agency. The DCF Procurement Manager once pursued a standard DSA, but it did not get anywhere. State and federals rules would have to change to make this work.
Interagency Data Sharing Agreement
Between
Department of Children and Families
And
Click here to enter name of agreement agency

This Agreement is made and entered into by and between the Florida Department of Children and Families (hereinafter “DCF” or the “Department”) and Click here to enter name of agreement agency.

I. Purpose
The purpose of this Agreement is to establish the terms and conditions by which the Department of Children and Families agrees to provide Click here to enter text.

The purpose of the data release is to Click here to enter text.

II. Legal Authority

III. Definitions
A. Agreement Coordinators – the individuals appointed by the signatories as responsible for compliance with the activities identified herein.
B. Data Exchange – A process for taking data structured under a source database and mapping it to a target database, so that the target data is an accurate representation of the source data.
C. Covered Data - data covered by federal or state laws or regulations.

IV. Implementation
A. Click here to enter name of agreement agency agrees to provide the Department with a list of categorical data elements that encompass specific data it wishes to obtain from Click here to enter name of system. The list of data elements is incorporated into this document as Exhibit “A,” Click here to enter name of document.

   1. Any revisions to Exhibit A shall require an amendment to this Agreement, attaching the revised Exhibit A thereto.

B. Click here to enter name of agreement agency agrees to restrict the transmission of the Covered Data received from the Department using secure file transfer protocols to
personnel who have a verifiable need to know in the performance of their official job duties.

C. Click here to enter name of agreement agency agrees to maintain a listing of personnel granted access privileges to the Covered Data pursuant to this Agreement and, upon request, make such information available to the Department. At a minimum, the list shall include the user’s name and title, User Identification (USERID), date access was granted/changed/deleted, and dates of initial security training and annual awareness training. This list shall be maintained at the office of the Click here to enter agreement agency and will also include the appropriate local technology officer’s name and contact information. Click here to enter name of agreement agency agrees to maintain the Covered Data for a period of five (5) years after access has been terminated or until administrative purposes have been served, whichever is longer.

D. Click here to enter name of agreement agency agrees to abide by IT Security Awareness training provided by the Department at [http://www.dcf.state.fl.us/admin/training.shtml](http://www.dcf.state.fl.us/admin/training.shtml) or an equivalent security training provided to IT security officers of the Click here to enter agreement agency.

E. Click here to enter name of agreement agency agrees that the Covered Data and Data Exchange obtained under this Agreement may not be disclosed by its employees verbally, electronically or in any other form except as specifically authorized by law or regulation. The Click here to enter agreement agency agrees:

1. That any Covered Data provided to Click here to enter name of agreement agency pursuant to this Agreement will be used only in the performance of official duties and shall be disclosed only for those purposes as defined in this Agreement.

2. That the Covered Data obtained shall be stored in a place physically secure from access by unauthorized persons.

3. To safeguard access to the Covered Data in such a way that unauthorized persons cannot view, print, copy or retrieve the information by any means.

4. That Click here to enter name of agreement agency shall instruct all staff, employees, and personnel with access to the Covered Data including the safeguards and requirements of this Agreement, and the provisions specified in Chapters 71A-1 and 71A-2 of the Florida Administrative Code as well as Chapters 39, 119, 812, 815, 817, 839 or 877, Florida Statutes and all applicable federal requirements. Initial and annual refresher IT Security Awareness training shall be required and documented.

5. That the confidentiality requirements of the Covered Data subject to this Agreement shall survive the expiration or termination of this Agreement.
6. To adhere to the confidentiality requirements stated herein, and promptly notify the Department within twenty-four (24) hours of any breach of security related to Covered Data in their possession. To be responsible for full compliance with section 817.5681, F.S., if applicable, in the event of a breach of security concerning confidential personal information in its possession received from one another, including but not limited to, providing notification to affected persons. To provide any such breach notification, if applicable, to the Department for prior review and approval of the contents of the notice.

F. The Department agrees to provide Click here to enter text

G. Click here to enter name of agreement agency shall ensure the adequacy of security controls for collecting, processing, transmitting and storing of Covered Data in leased, procured or developed systems and technologies, including sub-components as long as the Covered Data exists in the systems. In any developed system or technology or subcomponent thereof, including views, prints or copies of the Covered Data, a notice shall be provided to the user that the Covered Data is confidential and that users of the system shall be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. On-line systems shall require an acknowledgement and all views and prints shall contain the same statement. The violations of such confidential information security are addressed under Chapters 39, 119, 812, 815, 817, 839, or 877, Florida Statutes, and applicable Federal laws.

H. The following summary of key security standards is applicable to the Covered Data, in accordance with federal or state laws or regulations. The following list is not intended to be, and is not, exhaustive. Click here to enter name of agreement agency must comply with all security requirements related to Covered Data provided to, or collected by, Click here to enter name of agreement agency acting on behalf of the Department. Further, Click here to enter name of agreement agency’s employees, subcontractors, agents, or other affiliated third party persons or entities, as well as contracted third parties, must meet the same requirements of Click here to enter name of agreement agency under this Agreement and all amendments thereto with the Click here to enter name of agreement agency’s employees, subcontractors, agents, contractors or other affiliated persons or entities and shall incorporate the terms and conditions of this Agreement into any contractual relationships currently existing or existing in the future.

1. Access Controls:
   a. Viewing and modification of Covered Data must be restricted to authorized individuals as required for business related use.

   b. Unique authorization is required for each person permitted access to Covered Data and access must be properly authenticated and recorded for audit purposes, including HIPAA, Payment Card Industry (PCI), and Criminal Justice Information Services (CJIS) audit requirements.

   c. Access to all Covered Data provided to Click here to enter name of agreement
agency’s employees, subcontractors, contractors, agents, or other affiliated persons or entities must meet the same requirements of the

Click here to enter name of agreement agency under this Agreements and all amendments thereto with same and shall incorporate the terms and conditions of data security in the access authorization.

d. User access to Covered Data must be disabled within 24 hours after termination from employment or other change in employment where access to this data is no longer needed. User access must also be disabled after forty-five (45) days of inactivity.

2. Copying/Printing (applies to both paper and electronic forms):
   a. Covered Data should only be printed when there is a legitimate need.
   b. Copies must be limited to individuals authorized to access the Covered Data.
   c. Covered Data must not be left unattended.

3. Network Security:
   a. All electronic communication including, but not limited to, Covered Data between
      Click here to enter name of agreement agency and the Department shall use compatible, industry standard Secure File Transfer Protocol software, using data encryption or a Virtual Private Network connection to ensure a secure file transfer at no additional cost to the Department.
   b. Covered Data must be protected with a network firewall with “default deny” rule set required.
   c. Servers hosting the Covered Data cannot be visible to the entire Internet, nor to unprotected subnets.

4. Physical Security (Servers, laptops and remote devices on which Covered Data is stored). For purposes of these standards, mobile devices must be interpreted broadly to incorporate current and future devices, which may contain or collect Covered Data:
   a. The computing device must be locked or logged out when unattended.
   b. Servers must be hosted in a secure data center hardened according to relevant security standards, industry best practices, and department security policies.
   c. Physical access to servers containing Covered Data must ensure physical access is monitored, logged, and limited to authorized individuals at all times.
   d. Routine back-up of Covered Data is required and must be stored in a secure off-site location.

5. Remote access to systems hosting Covered Data:
   a. Remote access to Covered Data must be restricted to the local network or a secure virtual private network.
   b. Unauthorized remote access to Covered Data by third parties is not allowed.
   c. Access to Covered Data by all third parties must adhere to the requirements of this Agreement.

6. Data Storage:
   a. Storage of Covered Data on a secure server in a secure data center according to
relevant security standards, industry best practices, and Department security policies is required.

b. Covered Data stored on individual workstations or mobile devices must use full disk encryption with passwords. All mobile devices within the environment must have full disk encryption. If Covered Data is kept on the mobile device, any media, including flash cards, memory sticks, or external hard drives must be encrypted and stored in a secure location when not in use.

c. Covered Data is not to be transmitted through e-mail or social networking sites unless encrypted and secured with a digital signature.

7. Antivirus protection shall be utilized on all mobile devices, workstations, and servers to safeguard the confidentiality and integrity of Covered Data. At a minimum, antivirus signatures shall be updated daily with full disk scans performed every two weeks.

V. Costs

VI. Duration and Designation of Agreement Coordinators

A. This Agreement shall become effective on the last date of signature by the Parties and will terminate one year from said date, unless renewed or terminated. This Agreement may be renewed for two consecutive one-year terms upon the completion of the attached “Department of Children and Families Contract Monitoring Worksheet” (Exhibit “B”). To be eligible for renewal, the Contract Monitoring Worksheet must be completed by Click here to enter name of agreement agency by each contract anniversary.

B. This Agreement may be renewed in writing with appropriate modifications as agreed upon by the Parties.

C. This Agreement replaces Click here to enter name of previous agreement or delete section, if none and incorporates all prior negotiations, interpretations, and understandings between the Parties. The Agreement may be mutually terminated by written agreement of the parties or unilaterally by either party, without cause, provided the terminating party serves the other party’s Agreement Coordinator with written notice of an intent to terminate the Agreement in no less than thirty (30) days from the date such notice is sent. Either Party may terminate this Agreement for cause, without prior notice or warning, effective immediately upon written notice.

D. The Agreement Coordinators for this Agreement are:

Click here to enter name of agreement agency’s contact coordinator:
Click here to enter name of coordinator
Address line 1
Address line 2
City, State Zip
Email address
Phone number
The Department’s Agreement Coordinator:
Click here to enter name of coordinator
Address line 1
Address line 2
City, State Zip
Email address
Phone number

VII. Amendments and Changes
A. With the exception of changes to Agreement Coordinator designations (Section V. D.) any changes, alterations, deletions, or additions to the terms set forth in this Agreement must be by written amendment executed by all Parties. Changes to Section III. A. shall be accomplished as provided therein, changes to Section V. D. may be accomplished by providing email change notification that is acknowledged by both Parties.

B. The Parties agree to follow and be bound by the terms and conditions of any policy decisions or directives from the federal and state agencies with jurisdiction over the use of the data contained herein upon receipt of written notice directing that such rules, policy decisions, or directives apply to this Agreement.

VIII. Inspection of Records
Click here to enter name of agreement agency shall permit the Department or other state and federal representatives, or their designees, to conduct inspections described in this paragraph, or to make on-site inspections of records relevant to this Agreement to ensure compliance with any state and federal law, regulation, or rule. Such inspections may take place with notice during normal business hours wherever the records are maintained. Click here to enter name of agreement agency shall ensure a system is maintained that is sufficient to permit an audit of Click here to enter name of agreement agency’s compliance with this Agreement and the requirements specified above. Failure to allow such inspections constitutes a material breach of this Agreement.

IX. Liability
It is understood that neither party to this Agreement is the agent of the other and neither is liable for the wrongful acts or negligence of the other. Each party shall be responsible for its negligent acts or omissions and those of its officers, employees, or agents, howsoever caused, to the extent allowed by law and without waiving the limits of sovereign immunity.
A. Department of Children and Families

Office of General Counsel

By:___________________________                  By:___________________________
Signature                                                                 Signature

___________________________               ___________________________
Name/Title                                                               Name/Title

___________________________               ___________________________
Date                                                                   Date

Program Office

By:___________________________                  By:___________________________
Signature                                                                 Signature

___________________________               ___________________________
Name/Title                                                               Name/Title

___________________________               ___________________________
Date                                                                   Date

By:___________________________                  By:___________________________
Signature                                                                 Signature

___________________________               ___________________________
DCF CIO                                                                  Name/Title

___________________________               ___________________________
Date                                                                   Date
Contract ID: ___________________________   Date: ___________________________
   Completed By: _________________________

Notes

Sections IV.A., Validate that the “List of Data Elements” is current.

Section IV. B., Validate that Click here to enter text restricts the transmission of the data received from the Department to personnel who have a verifiable need to know in the performance of their official duties.

Section IV. C., Validate that Click here to enter text maintains a listing of personnel granted on-line access privileges to Department provided data under this agreement and, upon request, will make such information available to the Department. At a minimum list includes the user’s first and last name, User Identification (USERID), date access was granted/changed/deleted, dates of initial security training and annual awareness training that was provided as well as the appropriate court security officer’s name, email and phone number. Also validate that Click here to enter text will maintain this data for a period of 5 years after access has been terminated or until administrative purposes have been served, whichever is longer.

Section IV. D., Validate that Click here to enter text has abided by the Department’s security policies and training provided by the Department.

Section IV.E.1., Verify that Click here to enter text ensures that the information and the source of the information obtained under this Agreement is not re-disclosed verbally, electronically or in any other forms except as specifically authorized by law or regulation.

Section IV.E.2., Validate that the information provided by the Department is only used in the performance of employee official public duties and shall be disclosed only for those purposes as defined in the Agreement.
Section IV.E.3., Validate that the information obtained under this agreement is stored in a place physically secure from access by unauthorized persons.

Section IV.E.3., Validate that access to the confidential information is safeguarded in such a way that unauthorized persons cannot view, print, copy or retrieve the information by any means.

Section IV.E.4., Validate that Click here to enter text has instructed all personnel granted access to the confidential information provided by the Department regarding the confidential nature of the information, the safeguards and requirements of this Agreement and the provisions specified in Sections 443.171(5) and 443.1715, F.S. and 20 CFR Part 603.9. Initial and annual refresher instruction shall be documented.

Section IV.E.5., Validate that Click here to enter text will fully and promptly report any infraction of these requirements to the respective contacts specified in Section V. D. of this Agreement. Further validate that Click here to enter text recognizes that the confidentiality requirements of the data subject to this Agreement shall survive the expiration or termination of this Agreement.

Section IV.E.6., Validate that Click here to enter text agrees to promptly notify the Department of any breach of security related to Department provided confidential information in their possession. Further validate that Click here to enter text agrees to be responsible for full compliance with section 817.5681, F.S., if applicable, in the event of a breach of security concerning confidential personal information in their possession received from one another, including but not limited to, providing notification to affected persons.

Section IV.E.6., Validate that Click here to enter text agrees to provide any such breach notification, if applicable, to the Department for prior review and approval of the contents of the notice.

Section IV. H.1.a., Validate that Click here to enter text has not modified any of the data provided by the Department.

Section IV. H.3., Validate that Click here to enter text complies with State of Florida network security requirements specified in Florida Administrative Code 71A-2.006, Network Security.
10.3 APPENDIX 3 – DETAILS ON THE EVOLUTION OF THE CHILDREN’S AUTOMATED TRACKING SYSTEM (CATS) IN KENTUCKY

The following provides detailed information on the development of the Children's Automated Tracking System (CATS) in Kentucky. It was included because it may help in spurring some ideas on initiatives OCW may want to undertake.

The Kentucky General Assembly created the Citizen Foster Care Review Boards (CRCRBs) in 1982 in response to federal legislation aimed at decreasing the amount of time children spend in foster care. CRCRB volunteers are appointed by their chief Family Court or District Court judge to review the cases of children placed in the custody of the Cabinet for Health and Family Services due to dependency, neglect, or abuse. Volunteers regularly review each child’s case with a particular focus on the out-of-home placement and the permanency plan established by the Cabinet. Based on information obtained from the reviews, the volunteer makes recommendations to the judge to ensure the child is placed in a safe and permanent home in a timely manner.

The Department of Community-Based Services (DCBS) was formed within the Cabinet for Families and Children in 1998 to give local offices more decision-making authority and the ability to collaborate more effectively with other community service providers. The Cabinet for Families and Children and the Cabinet for Health Services were consolidated in 2004. The department provides family support; child care; child and adult protection; eligibility determinations for Medicaid and food benefits; and administration of an energy cost assistance program. The department administers the state foster care and adoption systems and recruits and trains parents to care for the state's children who are waiting for a permanent home. With offices in every county, DCBS provides services and programs to enhance the self-sufficiency of families; improve safety and permanency for children and vulnerable adults; and, engage families and community partners in a collaborative decision-making process.

Data are exchanged between the software systems supporting these departments. CATS (described above) shares data with the Worker Information System (TWIST), Kentucky's state automated child welfare information system (SACWIS). IT also shares data with the DCBS Private Child Care (PCC) Tracking System. DCBS also collaborates with the Department for Mental Health and Mental Retardation Services on information system issues that address co-customer needs.

TWIST includes extensive demographic and longitudinal data on children, families and foster parents and tracks permanency goals and placements for all children. The DCBS PCC Tracking System provides DCBS an accurate listing of private resource homes as well as the number of placement moves per child within an agency.

The Administrative Office of the Courts (AOC) and DCBS collaborated to form a Data Sharing Workgroup. The workgroup meets bimonthly and established a strategic plan to address data sharing issues, including the standardization of terminology, data meaning, and case identification and tracking options. In addition to this workgroup, the AOC recently partnered with the Department for Behavioral Health, Developmental and Intellectual Disabilities
(DBHID) and DCBS regarding a triangular approach to working with substance-using parents. Since each system interfaces with the same parents, collaboration is necessary to ensure that services are not duplicated and data are collected and shared in a manner that benefits all systems.
10.4 Appendix 4 – Data Governance Resources and Staffing

The following lists details regarding key desired state data governance roles including skills profiles and interactions with various peers, superior, and subordinate entities.

**Data Governance Leadership Committee**

**Description:** Executive oversight of data ownership, governance, quality, and controls. The Leadership Committee champions data governance as a strategic priority of the corporation. This committee advises the Data Governance Managers on prioritization and scope of data specific initiatives and manages corporate expectations regarding enterprise data management maturity and roadmap.

**Key Responsibilities:**

- Provide guidance to the data quality organization
  - Define agency strategies
  - Provide information regarding agency changes that have an impact on data quality
  - Approve and set priorities for areas of focus and for identified data quality improvement projects
  - Approve changes to the governance framework including changes to data governance practices, standards, measures, roles, responsibilities and processes
  - Arbitrate competing interests
  - Set timelines to meet data quality milestones
  - Make final decisions regarding data quality issues the Management layer is unable to resolve

- Communicate data quality related issues to the organization
  - Champion the importance of data quality throughout the company
  - Communicate issues or requests with the data governance organization
  - Communicate status of data quality initiatives and projects to others throughout the company
  - Communicate results of internal data quality and source audits and surveys
Key Interactions:

- Communicate with Executive Steering Committee to align with DCF vision
- Communicate to Subject Area Data Managers and IT Center of Excellence Managers on data quality issues and projects.

<table>
<thead>
<tr>
<th>Contact (indicate if inside or outside)</th>
<th>Reason for Contact</th>
<th>Frequency of Contact (Daily, Weekly, Monthly)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Governance Leadership Committee</td>
<td>Coordinate customer strategy, communicate data related issues</td>
<td>Monthly</td>
</tr>
</tbody>
</table>

Important Traits:

- Enterprise perspective
- Commitment to managing data as a corporate asset
- Authority to make final decisions
- Facilitation and arbitration skills
- Drive accountability for data quality to the appropriate teams/people
- Representation from various parts of the organization
  - Finance
  - HR
  - Policy
  - IT
  - Inter-Agency

**Data Governance Manager**

**Description:** The Data Governance Manager is the tactical management arm of the data governance framework. This person or team are independent of any work group, and act as primary facilitator and coordinator of data governance activities.

**Key Responsibilities:**

- Tracks data governance action items, issues and priorities
- Guides the Stewardship teams through the data governance practices and processes and facilitates issue resolution around the data governance framework
- Captures Stewardship team feedback and provides ongoing process improvement activity
- Maintains List of Subject Areas, Managers, Data Stewards, and Subject Area Stakeholders
- Logs Issues related to Subject Area Data and provides to Data Stewards
- Manages the final Repository of Subject Area Agency data requirements and data mappings
- Track Data Governance Process change requests, conduct process gap analysis and provide recommendations
- Updates Data Governance Process documentation
- Audits project level data governance deliverables to ensure that practices and standards are being met

**Key Interactions:**

<table>
<thead>
<tr>
<th>Contact</th>
<th>Reason for Contact</th>
<th>Frequency of Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Governance Leadership Committee</td>
<td>Coordinate client strategy, communicate data related issues</td>
<td>Monthly</td>
</tr>
<tr>
<td>Data Governance Managers</td>
<td>Coordinate cross domain dependencies and shared concerns</td>
<td>Monthly</td>
</tr>
<tr>
<td>Subject Area Data Steward and Agency/Dept. Leads</td>
<td>Awareness and decision processes related to accountable data sources; risks, issues, and progress related to data issues and processes</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

**Skills Required:**

- Knowledge of DCF Agency and culture
- Strong Leadership and communication skills. Conflict resolution
- Background in Data Management, data governance processes
- Project Management with an ability to identify and resolve issues
**Subject Area Data Manager**

**Description:** The Subject Area Data Manager provides leadership over a segment of enterprise data and the collection of Data Managers will result in governance over all enterprise data. It approves the data policies, standards, and guidelines pertaining to the accuracy, validity, and ownership of data and ensures decisions are aligned with the organization’s strategy.

**Key Responsibilities:**

- Guide the execution of subject area data quality and the specific processes that leverage this information
  - Understand the overall agency strategy and objectives
  - Maintain an enterprise view
  - Maintain a high-level understanding of end-to-end processes and systems landscape
  - Provide guidance on the data quality processes to the Data Stewards
  - Provide guidance enterprise process integration to the Agency Leads
  - Ensure Data Stewards and Agency Leads maintain an enterprise view
  - Ensure Data Stewards understand controls guidelines
  - Provide overall data quality guidelines, job aids and other processes
  - Communicate agency needs, requests, issues to the Data Governance Leadership Committee
  - Ensure agency unit requirements are fulfilled

- Monitor and manage compliance with data quality processes
  - Overall owner of customer data sourcing, usage, hygiene, archiving and agency rules as well as data-related standards, policies and measures
  - Ensure data quality metrics are set and collected appropriately
  - Ensure data quality processes and controls are adhered to by Data Stewards
  - Establish reporting tools, architecture, and processes for reporting data quality metrics vs. standards to the agency
  - Understand and communicate how agency and system changes may impact data quality
  - Take corrective action where there are compliance issues

- Monitor and manage changes in the subject area information platform
Overall subject matter expert of enterprise subject area processes are related and how they are integrated to tie to corporate goals
Understand and communicate how agency and system changes may impact subject area strategies

- Manage the relationship with the Data Governance Leadership Committee
  - Provide status and issues to the Data Governance Leadership Committee
  - Present agency cases for proposed projects
  - Escalate issues from Data Stewards as appropriate
  - Provide feedback to Data Stewards from the Data Governance Leadership Committee
  - Obtain buy-in for the practices, standards and measures from the Data Governance Leadership Committee and the agency

- Data quality improvement projects
  - Work with the agency in identifying subject areas requiring data quality improvements
  - Work with Data Stewards or the agency in developing ROI based agency cases
  - Assist with planning
  - Assist in resolving agency integration issues, when possible
  - Escalate issues to Data Governance Leadership Committee appropriate

**Key Interactions:**

- Manage Agency Leads and Data Stewards on day-to-day activities regarding data quality and subject area process issues and projects
- Communicate with the Data Governance Leadership Committee to align customer data and processes with the overall customer strategy

<table>
<thead>
<tr>
<th>Contact (indicate if inside or outside)</th>
<th>Reason for Contact</th>
<th>Frequency of Contact (Daily, Weekly, Monthly)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Governance Leadership Committee</td>
<td>Coordinate customer strategy, communicate data related issues</td>
<td>Quarterly</td>
</tr>
<tr>
<td>IT Personnel</td>
<td>Receive updates on projects in progress, set priorities</td>
<td>Daily</td>
</tr>
<tr>
<td>Contact</td>
<td>Reason for Contact</td>
<td>Frequency of Contact</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>External Vendors</td>
<td>Contract negotiations / management, systems planning</td>
<td>Monthly</td>
</tr>
<tr>
<td>DCF</td>
<td>Privacy planning, information sharing, ensuring initiative / project alignment between DCF / DCF</td>
<td>Weekly</td>
</tr>
<tr>
<td>Purchasing / IT Contracts</td>
<td>Contract renewal, development of statements of work</td>
<td>Monthly</td>
</tr>
<tr>
<td>DCF Managers</td>
<td>Consulting on projects</td>
<td>Weekly</td>
</tr>
<tr>
<td>Legal Council</td>
<td>Reviewing privacy legislation</td>
<td>Monthly</td>
</tr>
<tr>
<td>Industry Experts / Counterparts at other Financial Institutions</td>
<td>Discussing best practices</td>
<td>Monthly</td>
</tr>
<tr>
<td>Development and Maintenance Manager</td>
<td>Agency cases for uplift projects, break-fix/enhancement prioritization</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

Skills Required:

- **Project / Program Management Skills**
  - Good understanding of subject area agency processes
  - Ability to understand and communicate the overall agency strategy and objectives
  - Ability to identify impacts of agency or system changes on processes
  - Ability to set priorities with the Data Stewards and Agency Leads
  - Ability to identify and manage issues
  - Ability to clearly define action items, owners of action items, timelines, and accountability
  - Ability to perform work planning tasks (aggregates multiple work plans, understand resource needs, etc.)

- **Core Skills**
  - Strong functional and analytical skills
  - Problem solving skills
 › Solutions-oriented thinking
 › Ability to break complex areas down into manageable components
 › Tactically focused to execute
 › Ability to provide logical and reasonable next steps
 › Strong knowledge and skills in coaching, teaching, guiding techniques
 › Negotiation skills
 › Conciliation skills
 › Facilitation skills
 › Good Written / Verbal Communication
   - Solid listening skills to be able to understand the agency and customer needs, priorities, issues, etc.
   - Ability to effectively communicate based on the audience (i.e., what are they interested in, the level of detail, the medium used)
   - Ability to communicate effectively through multiple channels

▪ Other Important Traits
 › Highly respected individual
 › Committed to managing subject area data and related processes

▪ Subject Matter Expertise
 › Understanding of subject area processes and how data are used within them.
 › Understanding of subject area data and best practices in data management

**Data Steward**

**Description:** The Data Steward provides subject matter expertise on data related issues. This role is also responsible for defining agency rules around data integration and measuring and maintaining data quality.

**Key Responsibilities:**

▪ Standards and baseline of data quality
▪ Aid in the development of data quality practices and standards for subject areas
▪ Aid in the development of data quality metrics to be used in measuring the level of data quality
▪ Determine feasibility of obtaining appropriate information needed to report measures
▪ Obtain a baseline measurement of data quality based on the measures and standards developed
- Communicate and champion data quality practices, standards, measures and baseline to the agency and application stewards
- Monitor and manage data quality
  › Establish reporting mechanisms and timeframes to report data quality practices, standards and measures to the agency
  › Monitor data quality in the end-to-end processes, applications, and reports
- Propose data quality improvement projects
  › Identify need
  › Determine root causes of data issues
  › Develop plans to resolve issues
  › Help construct agency case
- Manage data quality improvement projects
  › Work with IT Application Personnel to implement data quality standards
  › Manage implementation of data quality measures reports
  › Resolve agency integration issues
  › Escalate issues to Data Manager as appropriate
- Communicate changes from the Data Governance Leadership Committee and the Data Manager
  › Understand future agency or system changes
  › Communicate to affected users
  › Communicate to affected Application Managers

**Key Interactions:**

- Collaborate with Data Manager on customer data quality improvement projects
- Communicate with DCF end-users to provide subject area data expertise and resolve subject area data-related issues

<table>
<thead>
<tr>
<th>Contact</th>
<th>Reason for Contact</th>
<th>Frequency of Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Managers, supervisors &amp; personnel</td>
<td>Task prioritization, specifications approval, work scheduling &amp; coordination, resource management</td>
<td>Daily</td>
</tr>
<tr>
<td>Contact</td>
<td>Reason for Contact</td>
<td>Frequency of Contact</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Data Stewards</td>
<td>Strategy, planning, cooperative decision making</td>
<td>Daily</td>
</tr>
<tr>
<td>Agency Line Managers</td>
<td>Discuss the efforts of the Tech Team, core support tickets, and prioritization</td>
<td>Weekly</td>
</tr>
<tr>
<td>External Vendors</td>
<td>Project management, scheduling, etc.</td>
<td>Weekly</td>
</tr>
<tr>
<td>Agency Leads</td>
<td>Break-fix/Enhancements ticket management</td>
<td>Daily</td>
</tr>
<tr>
<td>DCF End-Users</td>
<td></td>
<td>Daily</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>Issue resolution, UAT testing</td>
<td>Weekly</td>
</tr>
<tr>
<td>IT Data Architects</td>
<td>Logical Data Model maintenance</td>
<td>Monthly</td>
</tr>
<tr>
<td>Legal/Privacy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Skills Required:**

- **Personal attributes**
  - Highly respected individual
  - Committed to managing data as an asset
- **Core skills**
  - Negotiation
  - Conciliation
  - Facilitation
  - Persuasion
  - Written / Verbal Communication
- **Monitor and manage data quality (subject matter expertise)**
  - Data quality
  - Costs of poor data
  - Deep understanding of the agency requirements for the subject area
  - Deep understanding of the agency rules and data for the subject area
  - Detailed understanding of end-to-end processes and applications using the data
- **Project management skills**
- **Enterprise knowledge**
  - Enterprise perspective
  - Understanding of the agency strategy and objectives
  - High-level understanding of end-to-end processes and systems landscape
10.5 Appendix 5 – Data Governance Processes

Major data governance processes that leverage the roles and interactions described in Appendix 1 are documented here.

10.5.1 Summary of Data Governance Process Flows

The following tables summarize the standard operating procedures that the governance organization would perform in order to stay compliant and aligned with agency data governance practices, standards and measures.

<table>
<thead>
<tr>
<th>Manage Data Governance Framework</th>
<th>Process #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1</td>
<td>Assign stewardship to subject area data</td>
</tr>
<tr>
<td></td>
<td>1.2</td>
<td>Manage changes to the data governance framework</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manage Subject Area Data</th>
<th>Process #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.1 &amp; 2.3</td>
<td>Manage break-fix / maintenance / enhancement requests</td>
</tr>
<tr>
<td></td>
<td>2.2 &amp; 2.4</td>
<td>Manage new project requests</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>Manage Data Pulls and Extract Requests</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manage Subject Area Data Quality</th>
<th>Process #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.1</td>
<td>Audit Subject Area Data</td>
</tr>
<tr>
<td></td>
<td>3.2</td>
<td>Resolve user inquiries into Subject Area Data Quality</td>
</tr>
</tbody>
</table>
10.5.2 MANAGE GOVERNANCE FRAMEWORK

10.5.2.1 ASSIGN STEWARDSHIP TO SUBJECT AREA DATA

Pre-Conditions

- DCF End-User has identified a need to govern a data subject area
- Subject area stewardship not defined

Post-Conditions

- The change to the governance framework is updated within the appropriate document and communicated to the organization

Figure A5-1 – Assign Stewardship to Subject Area
10.5.2.2 MANAGE CHANGE TO THE DATA GOVERNANCE FRAMEWORK

Pre-Conditions

- DCF End-User has identified a need for a change to a component in the governance framework

Post-Conditions

- The change to the governance framework is updated within the appropriate document and communicated to the organization
Figure A5-2 – Manage Data Governance Framework Change
### 10.5.3 Manage Subject Area Data

#### 10.5.3.1 Manage Break-Fix / Maintenance / Enhancement Requests

**Pre-Conditions**
- DCF End-User has identified a need for data fix
- DCF End-User has identified a need for a production-fix(maintenance) or enhancement

**Post-Conditions**
- Break-Fix / Maintenance / Enhancement Request is approved and project is initiated
Figure A5-3 – Manage Maintenance and Enhancement Requests
10.5.3.2 **MANAGE NEW PROJECT REQUESTS**

**Pre-Conditions**
- DCF has received a request for a new data uplift or data quality improvement project.

**Post-Conditions**
- New project is initiated
Figure A5-4 – Manage New Project Requests
10.5.3.3 MANAGE DATA PULLS AND EXTRACT REQUESTS

Pre-Conditions
- End-User has identified a need for subject area data

Post-Conditions
- End-User has received their requested data
10.5.4 MANAGE SUBJECT AREA DATA QUALITY

10.5.4.1 AUDIT SUBJECT AREA DATA

Figure A5-6 – Audit Subject Area Data Quality
10.5.4.2 RESOLVE USER INQUIRIES INTO SUBJECT AREA DATA QUALITY

Figure A5-7 – Resolve Data Quality User Inquiries
10.6 Appendix 6 – Data Acquisition Playbook

The steps necessary to accomplish data sharing and data acquisition are listed below. It is presented first as a checklist, then a set of process flows to execute the checklist. Lastly, there is a table describing each task and decision point in the process flows.

10.6.1 Data Sharing and Data Acquisition Checklist:

The checklist below includes a hierarchical list of steps that, once complete, satisfy the step in the next higher level of the hierarchy. Once all sub-tasks are complete within a hierarchy, the higher-level task is complete.

<table>
<thead>
<tr>
<th>Complete?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**A. Identify the need**

1. Know the business objectives behind the data being requested; identify what the data sharing is meant to achieve
   
   i. Ensure everyone understands why the data are needed and how it will be used
   
   ii. Ensure the context and scope is clearly defined and understood
   
   iii. Determine if the objective can be achieved without sharing personal data

**B. Document the metadata to ensure a clear understanding of the data**

Metadata is data that describes other data. Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. In databases, metadata defines data elements and attributes (name, data type, size, description, etc.); data could be registered about structures and records as well (length, columns and fields).

1. Clearly define the specific data elements needed

2. Identify the data characteristics (e.g., health, financial, etc.)

3. Group new data elements into subject areas (data categorization)

   Data classification is the process of sorting and categorizing data into various types, forms or any other distinct class. Data classification enables the separation and classification of data according to data set requirements for various business or personal objectives. It is mainly a data management process.

**C. Identify the source**
<table>
<thead>
<tr>
<th>COMPLETE? (✓)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Identify the best source to acquire the data (the Data Sharing Organization, or DSO)</td>
</tr>
<tr>
<td></td>
<td>2. Determine if a DSA is already in place with the DSO</td>
</tr>
<tr>
<td></td>
<td>3. Determine if the new data elements are already covered under the existing DSA</td>
</tr>
<tr>
<td></td>
<td>4. If they are not covered:</td>
</tr>
<tr>
<td></td>
<td>i. Meet with the DSO</td>
</tr>
<tr>
<td></td>
<td>ii. Clearly articulate the reason for requesting this specific data from the specific DSO</td>
</tr>
<tr>
<td>D. Communicate</td>
<td>1. Develop the appropriate communication channels to ensure that the agreement and the consequences of sharing the data are known by the relevant people</td>
</tr>
<tr>
<td></td>
<td>2. Understand the DSO’s current data sharing policies, practices, and procedures</td>
</tr>
<tr>
<td></td>
<td>3. Determine if the DSO has an existing DSA template</td>
</tr>
<tr>
<td></td>
<td>4. Define the case and the justification for sharing the data</td>
</tr>
<tr>
<td></td>
<td>5. Assess the benefits and risks in sharing the data</td>
</tr>
<tr>
<td></td>
<td>6. Assess the DSO technical infrastructure and support to exchange data</td>
</tr>
<tr>
<td></td>
<td>i. Digital availability and structure of the data</td>
</tr>
<tr>
<td></td>
<td>ii. Data exchange communication protocols</td>
</tr>
<tr>
<td></td>
<td>7. Identify business process or IT modifications required to support data exchange</td>
</tr>
<tr>
<td></td>
<td>i. Level of Effort – how much work is required from each side to design, develop, and implement the data exchange</td>
</tr>
<tr>
<td></td>
<td>ii. Technical resource support requirements</td>
</tr>
<tr>
<td></td>
<td>iii. Schedule</td>
</tr>
<tr>
<td>COMPLETE?</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>✔</td>
<td>iv. Budget</td>
</tr>
<tr>
<td></td>
<td>v. Funding</td>
</tr>
<tr>
<td></td>
<td>8. Ensure the responsibilities of individual members of staff clearly defined and understood</td>
</tr>
<tr>
<td></td>
<td>9. Ensure the safety, security and confidentiality of the data during and after the exchange</td>
</tr>
<tr>
<td></td>
<td>10. Ensure a process is in place to feedback any problems in relation to transmission, access, data quality, etc.</td>
</tr>
<tr>
<td></td>
<td>11. Establish change management processes (e.g., version control)</td>
</tr>
<tr>
<td></td>
<td>12. Define retention and archival requirements</td>
</tr>
</tbody>
</table>

E. Identify the obstacles

1. Identify the legal limitations/ramifications
   i. Understand the Florida statutes and regulations associated with sharing the data
   ii. Understand the federal statutes and regulations associated with sharing the data

2. Identify any Internal Review Board (IRB) requirements

3. Identify the security requirements

F. Develop the Data Sharing Agreement (DSA)

The DSA should be a living document that can easily be modified as changes in data requirements arise.

1. Include the appropriate content
   i. Purpose
   ii. Scope
   iii. Relevant Florida statutes and regulations
   iv. Authorizing parties and the process to obtain authorization
<table>
<thead>
<tr>
<th>COMPLETE? (✓)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>v. The reasons and justification for sharing the data</td>
</tr>
<tr>
<td></td>
<td>vi. Limitations to data use</td>
</tr>
<tr>
<td></td>
<td>vii. The specific data required</td>
</tr>
<tr>
<td></td>
<td>viii. Roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>ix. Data subject consent requirements</td>
</tr>
<tr>
<td></td>
<td>x. Data subject notification requirements</td>
</tr>
<tr>
<td></td>
<td>xi. Content defining the safety, security and confidentiality of the data during and after the exchange</td>
</tr>
<tr>
<td></td>
<td>xii. The frequency of the data exchange</td>
</tr>
<tr>
<td></td>
<td>xiii. Problem resolution processes and procedures</td>
</tr>
<tr>
<td></td>
<td>xiv. Compliance monitoring and review processes and procedures</td>
</tr>
<tr>
<td></td>
<td>xv. Data breach policies and procedures</td>
</tr>
<tr>
<td></td>
<td>xvi. Document termination reasons and procedures</td>
</tr>
<tr>
<td></td>
<td>xvii. Document an expiration/renewal schedule procedures</td>
</tr>
<tr>
<td></td>
<td>xviii. Data retention and archival requirements</td>
</tr>
<tr>
<td></td>
<td>2. Establish a timeline to process and finalize the DSA</td>
</tr>
</tbody>
</table>

**G. Data Acquisition**

<p>| 1. | Gain an understanding of the DSO’s metadata for the data being exchanged |
| 2. | Develop data profiling and data quality processes to ensure the DSO’s data files comply with the metadata |
| 3. | Establish the data encoding (e.g., ASCII, EBCDIC), format (e.g., fixed file, CSV, XML, web service), and exchange method (e.g., X12, NIEM, HL-7) |
| 4. | Establish the data exchange protocol (e.g., email, FTP/SFTP, brokered messaging) |</p>
<table>
<thead>
<tr>
<th>COMPLETE? (✓)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5. Implement the IT infrastructure (e.g. communication networks, IP addresses, data storage)</td>
</tr>
<tr>
<td></td>
<td>6. Implement security requirements</td>
</tr>
<tr>
<td></td>
<td>7. Implement retention and archival requirements</td>
</tr>
<tr>
<td></td>
<td>8. Test and revise all data acquisition processes until all expected results are achieved</td>
</tr>
<tr>
<td></td>
<td>9. Migrate all data acquisition processes to production</td>
</tr>
<tr>
<td></td>
<td>10. Design, Develop and Implement (DD&amp;I) the data acquisition models and processes need to satisfy the new business requirements</td>
</tr>
</tbody>
</table>

**Exhibit A6-1: Data Sharing and Data Acquisition Checklist**

**10.6.2 Data Sharing and Data Acquisition Playbook Process Flows:**

Below is the process flow version of the Data Sharing and Data Acquisition Playbook. It depicts the recommended step-by-step actions to take and decisions to make when trying to acquire data from an external agency.
Figure A6-2 – Identify Data Needs and Data Sources
Figure A6-3 – Develop DSA Addendum
Figure A6-4 – Develop New DSA
Figure A6-5 – Data Acquisition
### 10.6.3 Data Sharing and Data Acquisition Playbook Table:

The table below provides more descriptive information for each task and decision point in the process flows above.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>TASK</th>
<th>OWNER</th>
<th>DESCRIPTION</th>
<th>EXPECTED OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>A01</td>
<td>Determine the new Data Analytics outcomes needed to support new business requirements.</td>
<td>OCW</td>
<td>Document the analytical information needed to support a ROA metric.</td>
<td>A description of the information needed to measure the results of a ROA metric.</td>
</tr>
<tr>
<td>A02</td>
<td>Identify new data elements needed to support the new data analytics outcomes.</td>
<td>OCW</td>
<td>Document the data elements needed to clearly identify the subject of the metric and give a quantifiable measure of the metric.</td>
<td>A description of all the data elements needed to identify the subject and quantifiable outcome of a metric.</td>
</tr>
<tr>
<td>B01</td>
<td>Document metadata for each new data element.</td>
<td>OCW</td>
<td>Summarize basic information about data, which can make finding and working with particular instances of data easier.</td>
<td>A complete description for each data element to ensure a common understanding of each data element's meaning within OCW and outside OCW.</td>
</tr>
<tr>
<td>B02</td>
<td>Group new data elements into subject areas (data categorization).</td>
<td>OCW</td>
<td>Data categorization is the process of sorting and categorizing data into various types, forms or any other distinct class. Data classification enables the separation and classification of data according to data set requirements for various business or personal objectives.</td>
<td>A document grouping all data elements into categories to facilitate data acquisition.</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>C01</td>
<td>Determine the best data source organization for each data category.</td>
<td>OCW</td>
<td>Identify the department or agency that can best provide the data in a specific data category. For example, the Department of Juvenile Justice may be the best source of judicial information about a child.</td>
<td>Identification of the best source of data for each data category required to support data analytics outcomes.</td>
</tr>
<tr>
<td>C02</td>
<td>Does OCW already have a DSA in place with the DSO?</td>
<td>OCW</td>
<td>If a DSA is already in place, an addendum can be developed and the process to finalization should be quicker. If a DSA is not already in place, follow the processes to develop a new DSA.</td>
<td>Know if the process of developing and finalizing the DSA needs to start from scratch. If DSA is not in place EXECUTE STEPS STARTING AT E01</td>
</tr>
<tr>
<td>C03</td>
<td>If a DSA in place, are the data elements already covered? If a DSA in place, and the data elements are not already covered, Begin Develop DSA Addendum processes.</td>
<td>OCW</td>
<td>If the data elements are already covered, OCW can begin incorporating the new data elements into DA processes. If the data elements are not already covered, follow the processes to develop a DSA Addendum.</td>
<td>Know if any DSA addendum work is required. If data elements are not covered EXECUTE STEPS STARTING AT D01</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>C04</td>
<td></td>
<td></td>
<td></td>
<td>END CHECKLIST EXECUTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If a DSA in place, and the data elements are already covered, DSA development is not needed, Begin making the OCW business process and IT changes needed to include the new data elements.</td>
<td>The new data elements are available to OCW.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Design, Development and Implementation (DD&amp;I) of the DA models and processes need to satisfy the new business requirements.</td>
<td>Implement any new business processes required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OCW</td>
<td></td>
<td>› New data steward duties</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>› New data problem resolution processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Implement any new IT changes required</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>› New data models</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>› New data profiling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>› New data cleansing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>› New ETL</td>
</tr>
<tr>
<td>D01</td>
<td>Develop DSA Addendum</td>
<td>OCW</td>
<td>Complete the tasks steps E and F from the “Steps to Data Sharing and Data Acquisition” task list to ensure everything is properly documented in the addendum.</td>
<td>Any DSA terms or conditions that may need modification from step F of the “Steps to Data Sharing and Data Acquisition” task list.</td>
</tr>
<tr>
<td><strong>STEP #</strong></td>
<td><strong>TASK</strong></td>
<td><strong>OWNER</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>EXPECTED OUTCOME</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>D02</td>
<td>Develop an addendum to the existing DSA to include the new data elements and metadata.</td>
<td>OCW</td>
<td>Ensure that the steps A and B from the “Steps to Data Sharing and Data Acquisition” task list are completed and accounted for to fully develop the addendum.</td>
<td>A list of the new data categories and data elements needed from the DSO, along with each data element’s metadata.</td>
</tr>
<tr>
<td>D03</td>
<td>Meet with the data steward at the DSO to present and discuss the DSA addendum.</td>
<td>OCW</td>
<td>Consider the items under step D from the “Steps to Data Sharing and Data Acquisition” task list to make sure the proper things are being communicated to successfully finalize the DSA addendum.</td>
<td>An agreed upon DSA addendum that can be presented to the proper people for authorization.</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>D04</td>
<td>Meet with the DSO to define the steps required to adjudicate and get final disposition on the DSA addendum authorization.</td>
<td>OCW DSO</td>
<td>Develop a step-by-step task list to get final disposition on the DSA addendum. Try to set a target date to complete each task.</td>
<td>▪ A complete mapping of the data elements from the DSO that satisfy the list of data elements OCW is requesting ▪ A document management workflow of: › The tasks required to create the DSA addendum to DSO specifications › The DSO individuals that must approve the DSA addendum › The method(s) to check status along the work flow</td>
</tr>
<tr>
<td>D05</td>
<td>Submit the DSA addendum for approval</td>
<td>ESC DSO</td>
<td>“ESC” is the Data Governance Executive Steering Committee. It would be preferable for the authorizing person or people from the DSO to already be on the ESC. This would improve early communication and may expedite the entire DSA process.</td>
<td>Agreed upon DSA addendum submitted to the proper people for approval.</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>D06</td>
<td>Is the DSA addendum approved?</td>
<td>ESC DSO</td>
<td>DSA addendum approval/denial. If the DSA addendum is approved, and the data technical staff from OCW and the DSO can start working on data acquisition processes.</td>
<td>▪ Approval of the DSA addendum, allowing the actual data acquisition process to start ▪ Denial of the DSA addendum, in which case, alternatives must be determined If the DSA addendum is approved EXECUTE STEPS STARTING AT F01</td>
</tr>
<tr>
<td>D07</td>
<td>If the DSA addendum is not approved, Can the DSA addendum be revised to gain approval?</td>
<td>ESC DSO</td>
<td>Were revision suggestions made to gain approval for a denied DSA addendum? If the DSA addendum is not approved, OCW needs to determine if there is an alternative DSO for data acquisition. The process would start over from step C of the “Steps to Data Sharing and Data Acquisition” task list.</td>
<td>Know if the denied DSA addendum can be revised to gain approval. If the DSA addendum cannot be revised to gain approval EXECUTE STEPS STARTING AT C01 OCW needs to identify an alternative DSO.</td>
</tr>
<tr>
<td>D08</td>
<td>If the DSA addendum is not approved, and the DSA addendum can be revised to gain approval, Make the suggested revisions and resubmit for approval.</td>
<td>OCW DSO</td>
<td>Suggested revision need to be made to the DSA addendum to gain approval.</td>
<td>A revised DSA addendum resubmitted for approval. EXECUTE STEPS STARTING AT D05</td>
</tr>
<tr>
<td><strong>STEP #</strong></td>
<td><strong>TASK</strong></td>
<td><strong>OWNER</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>EXPECTED OUTCOME</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-----------</td>
<td>-----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>E01</td>
<td>Develop New DSA</td>
<td>OCW</td>
<td>Complete the tasks steps E and F from the “Steps to Data Sharing and Data Acquisition” task list to ensure everything is properly documented in the new DSA.</td>
<td>A new draft DSA that complies with all new standards and conditions.</td>
</tr>
<tr>
<td></td>
<td>Develop a new DSA that it is compliant with all new standards and conditions (e.g., legal, security, appropriate content).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E02</td>
<td>Include the new data elements and metadata.</td>
<td>OCW</td>
<td>Ensure that the steps A and B from the “Steps to Data Sharing and Data Acquisition” task list are completed and accounted for to fully develop the new DSA.</td>
<td>A list of the new data categories and data elements needed from the DSO, along with each data element’s metadata.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E03</td>
<td>Review the DSA with the ESC</td>
<td>OCW ESC</td>
<td>Present the draft DSA to the ESC for feedback. If the DSA is targeting a group that is not represented on the ESC, consider requesting them to join. This would improve early communication and may expedite the entire DSA process.</td>
<td>A draft DSA that the ESC agrees can be presented to the DSO.</td>
</tr>
<tr>
<td>E04</td>
<td>Does the ESC approve submitting the DSA to the DSO?</td>
<td>ESC</td>
<td>Determine if the DSA is ready to submit to the DSO. This does not ensure the DSA will be approved by the DSO. It would be preferable for the authorizing person or people from the DSO to already be on the ESC. This would improve early communication and may expedite the entire DSA process.</td>
<td>▪ Approval, allowing DSA submittal to the DSO. ▪ Denial, requiring revision before submitting the DSA to the DSO.</td>
</tr>
<tr>
<td>Step #</td>
<td>Task</td>
<td>Owner</td>
<td>Description</td>
<td>Expected Outcome</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>E05</td>
<td>If the ESC does not approve submitting the DSA to the DSO, Revise the DSA and resubmit to the ESC.</td>
<td>OCW</td>
<td>Make the revisions needed to get ESC approval to submit the DSA to the DSO.</td>
<td>A draft DSA that the ESC agrees can be presented to the DSO.</td>
</tr>
<tr>
<td>E06</td>
<td>If the ESC approves submitting the DSA to the DSO, Meet with the data steward at the DSO to present and discuss the DSA.</td>
<td>OCW</td>
<td>Consider the items under step D from the “Steps to Data Sharing and Data Acquisition” task list to make sure the proper things are being communicated to successfully finalize the DSA. To expedite the process, come to the meeting with a prepared DSA.</td>
<td>An agreed upon DSA addendum that can be presented to the proper people for authorization.</td>
</tr>
</tbody>
</table>
| E07   | Meet with the DSO to define the steps required to adjudicate and get final disposition on the DSA authorization. | OCW    | Develop a step-by-step task list to get final disposition on the DSA. Try to set a target date to complete each task. | ▪ A complete mapping of the data elements from the DSO that satisfy the list of data elements OCW is requesting  
▪ A document management workflow of:  
  › The tasks required to create the DSA to DSO specifications  
  › The DSO individuals that must approve the DSA  
  › The method(s) to check status along the work flow |
<table>
<thead>
<tr>
<th><strong>STEP #</strong></th>
<th><strong>TASK</strong></th>
<th><strong>OWNER</strong></th>
<th><strong>DESCRIPTION</strong></th>
<th><strong>EXPECTED OUTCOME</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>E08</td>
<td>Submit the DSA for approval</td>
<td>ESC DSO</td>
<td>“ESC” is the Data Governance Executive Steering Committee. It would be preferable for the authorizing person or people from the DSO to already be on the ESC. This would improve early communication and may expedite the entire DSA process.</td>
<td>Agreed upon DSA submitted to the proper people for approval.</td>
</tr>
<tr>
<td>E09</td>
<td>Is the DSA approved?</td>
<td>ESC DSO</td>
<td>DSA approval/denial. If the DSA is approved, and the data technical staff from OCW and the DSO can start working on data acquisition processes.</td>
<td>▪ Approval of the DSA, allowing the actual data acquisition process to start ▪ Denial of the DSA, in which case, alternatives must be determined</td>
</tr>
<tr>
<td>E10</td>
<td>If the DSA is not approved, Can the DSA be revised to gain approval?</td>
<td>ESC DSO</td>
<td>Were revision suggestions made to gain approval for a denied DSA? If the DSA is not approved, OCW needs to determine if there is an alternative DSO for data acquisition. The process would start over from step C of the “Steps to Data Sharing and Data Acquisition” task list.</td>
<td>Know if the denied DSA can be revised to gain approval. If the DSA cannot be revised to gain approval EXECUTE STEPS STARTING AT C01 OCW needs to identify an alternative DSO</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>E11</td>
<td>If the DSA is not approved, and the DSA can be revised to gain approval, Make the suggested revisions and resubmit for approval.</td>
<td>OCW DSO</td>
<td>Suggested revision need to be made to the DSA to gain approval.</td>
<td>A revised DSA resubmitted for approval. EXECUTE STEPS STARTING AT E08</td>
</tr>
</tbody>
</table>
| G01   | Data Acquisition  
Gain an understanding of the DSO's metadata for the data being exchanged. | OCW DSO | Review the DSO's metadata data and dictionary documentation to gain an understanding of the data being acquired. Have meetings to resolve any questions. | A documented understanding of the data characteristics of the data being acquired from the DSO so OCW can validate the data quality. |
| G02   | Develop data profiling and data quality processes to ensure the DSO's data files comply with the metadata. | OCW | Based on the data characteristics, develop automated process for data validation and exception reporting.  
Any processes described after this one (e.g., G03, G04, etc.) may have an impact on this work. | Automated processes that validate the quality of the data being received. |
<table>
<thead>
<tr>
<th>STEP #</th>
<th>TASK</th>
<th>OWNER</th>
<th>DESCRIPTION</th>
<th>EXPECTED OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>G03</td>
<td>Establish the data encoding (e.g., ASCII, EBCDIC), format (e.g., fixed file, CSV, XML, web service), and exchange method (e.g., X12, NIEM, HL-7).</td>
<td>OCW DSO</td>
<td>Data may be encoded differently on different computer platforms. It is important to know the data encoding to be able to interpret it properly. One needs to know the format and exchange method properly parse the data record into its data elements. If the DSO is already using specific methods for encoding, format and exchange, OCW may want to conform to those methods to make the data exchange easier for the DSO to implement.</td>
<td>Documented knowledge of the data file encoding, format and exchange method to make it possible to parse the data to validate data quality and metadata compliance. Implementation of the items needed to meet the requirements.</td>
</tr>
<tr>
<td>G04</td>
<td>Establish the data exchange protocol (e.g., email, FTP/SFTP, brokered messaging).</td>
<td>OCW DSO</td>
<td>Determine how the data file will be electronically transmitted by the DSO and received by OCW. If the DSO is already using specific protocol, OCW may want to conform to those methods to make the data exchange easier for the DSO to implement.</td>
<td>Documented knowledge to the data file transmission method. Implementation of the items needed to meet the requirements.</td>
</tr>
<tr>
<td>G05</td>
<td>Implement the IT infrastructure (e.g., communication networks, IP addresses, data storage).</td>
<td>OCW DSO</td>
<td>Determine the communication requirements to transmit the data from the sender to the receiver. Ensure the data can be stored once it is received.</td>
<td>Documented knowledge of the network communication and data storage requirements. Implementation of the items needed to meet the requirements.</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>G06</td>
<td>Implement security requirements.</td>
<td>OCW DSO</td>
<td>Make sure that all security protocols and procedures are in place to protect the privacy and confidentiality of individuals identified in the data.</td>
<td>Documented knowledge of the security requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Implementation of the items needed to meet the requirements.</td>
</tr>
<tr>
<td>G07</td>
<td>Implement retention and archival requirements.</td>
<td>OCW DSO</td>
<td>Understand the data retention and archival requirements stipulated in the DSA.</td>
<td>Documented knowledge of the retention and archival requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implement automated processes, as much as possible, to meet the requirements.</td>
<td>Implementation of the items needed to meet the requirements.</td>
</tr>
<tr>
<td>G08</td>
<td>Test and revise all data acquisition processes until all expected results are achieved.</td>
<td>OCW DSO</td>
<td>Test all processes developed and implemented as part of the data acquisition effort. Keep testing until all processes are achieving expected results.</td>
<td>Fully functional data acquisition processes supporting the sending and receiving and data files from the DSO to the OCW.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Knowledge that all functionality is meeting expected results and ready to migrate to a production state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Once this is done design, develop and implement (DD&amp;I) the DA models and processes need to satisfy the new business requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>EXECUTE STEPS STARTING AT C04</td>
</tr>
<tr>
<td>STEP #</td>
<td>TASK</td>
<td>OWNER</td>
<td>DESCRIPTION</td>
<td>EXPECTED OUTCOME</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>G09</td>
<td>Migrate all data acquisition processes to production.</td>
<td>OCW DSO</td>
<td>Move all processes developed and implemented as part of the data acquisition effort to a production IT state.</td>
<td>Everything developed as part of the data acquisition effort running is a repetitive consistent and accurate state.</td>
</tr>
</tbody>
</table>

**Figure A6-6 – Data Sharing and Acquisition Playbook**