Project Data Flow Diagram Change Summary Table

Version	Name	Date	Description
1.0.0	Hot Java	02/22/2020	Came up with level 1 data flow diagram rough draft
1.0.1	Cynthia Sustaita Jesus Gutierrez	02/22/2020	Sketched level 1.0 diagram on draw.io
1.0.2	Joaquin Hidalgo Cynthia Sustaita	02/23/2020	Identified nouns and verbs from RDD and Interview Report
1.0.3	Cynthia Sustaita Joaquin Hidalgo	02/23/2020	Added below and identified nouns and verbs from interview report Q&A section
1.0.4	Hot Java	02/24/2020	Sketched new data flow diagram based on Ben's feedback.
1.0.5	Cynthia Sustaita Joaquin Hidalgo Lauren Eagan Jesus Gutierrez	02/25/2020	Updated data flow diagram based on Elsa's feedback during her office hours
1.0.6	Cynthia Sustaita Lauren Eagan	02/26/2020	Identified nouns and verbs from risk matrix
1.0.7	Cynthia Sustaita Lauren Eagan Fernando Marquez	02/26/2020	Analyzed feedback provided by Elsa and updated diagram based on it. Changes include data flowing from a sink to a

			data store and error on output from findings to user management data store
1.0.8	Cynthia Sustaita	02/26/2020	Identified which verbs/nouns were used in our DFD. Created data dictionary for DFD data flowing
1.0.9	Cynthia Sustaita	02/27/2020	Added a data store for report details
1.1.0	Hot Java	03/05/2020	Updated DFD based on client's presentation feedback
1.1.1	Cynthia Sustaita Lauren Eagan Joaquin Hidalgo	03/07/2020	Updated DFD based on Elsa's feedback during 03/06 guidance meeting
1.1.2	Cynthia Sustaita Joaquin Hidalgo	03/07/2020	Created DFD Level 2. Updated DFD Level 2 based on Ben's feedback
1.1.3	Cynthia Sustaita Joaquin Hidalgo Fernando Marquez Lauren Eagan	03/25/2020	Updated DFD Level 2 based on Elsa's feedback
1.1.4	Cynthia Sustaita	05/17/2020	Updated DFD Level1 and 2 based on final presentation feedback

For the following list of verbs and nouns, we've highlighted the verb/noun that we identified to be used in our DFD. Additionally, some verbs/nouns will repeat for each of our resources, but they're still highlighted for each section. The duplicates are handled on the DFD itself.

RDD nouns:

- Cyber engagement/Event
- System
- Network scan
- Vulnerability Validation
- Penetration test
- Access control check
- Physical inspection
- Personnel interviews
- Reviews
- Cybersecurity status
- Final technical report
- PM
- Lead analyst
- Analyst
- Task
- Vulnerability
- Finding
- Mitigation
- Sub-task
- Screenshot
- Artifact
- Software
- Text
- Image
- Data
- Title
- Description
- Status
- Priority
- Due date
- Host IP
- Note
- Attachments

Verb phrases have been modified for abstraction and clarification purposes in our DFD

RDD verbs:

- Assign portions/requirements of a system to each analyst
- Give each task a priority
- Each task will be assigned to at least one analyst
- Add vulnerability/finding to the technical report
- Mark task as complete
- Document vulnerability/finding
- Share findings
- Analyst must provide a mitigation to the discovered vulnerability

- Software should also give the lead analyst insight into the progress of the predefined tasks
- Export findings to technical report
- Create/edit/delete tasks
- Relate finding to task
- System must allow analysts edit task’s status
- Create/edit/delete findings
- Associate finding to another finding
- Search for finding

Interview report nouns:

- System
- Data
- Analyst
- Lead analyst
- Hard drive
- Cyber engagement
- Project Manager
- Subject matter expert
- Record
- Chat system

Interview report verbs:

- lead analyst and analyst will share all data.
- The data will be stored in a hard drive and then archived.
- establishing the rules with team
- use their tools to gather findings
- share findings by collecting pictures, text and then syncing their data
- Communicate by chat

- Sort findings
- Sync data
- View event progress
- Receive past due task alert
- Export formatted technical report
- The lead analyst will create tasks based on the system testing plan that is given to CEAD from the PM and give each task a priority.

- Technical report
- Excel spreadsheet
- Subtask
- Findings are vulnerabilities
- Data point
- Client
- Report
- Task
- DDMMYYYY no slashes
- Notification
- Data

- Lead analyst receive updates to progress completed
- Lead analyst receive updates to progress findings
- Analyst will maintain record of what they have done

- Communicate within the system
- Export report
- Verify findings are true positives
- Team talks about if vulnerability or not
- Findings search by filter

- Everything will come out on report
- Task can be created without assignment
- Due date displayed

Risk Matrix nouns:

- ID
- Host name
- IP:Port
- Finding type
- Description
- Long description
- Status
- Posture
- IMP. Score
- CAT
- CAT Score

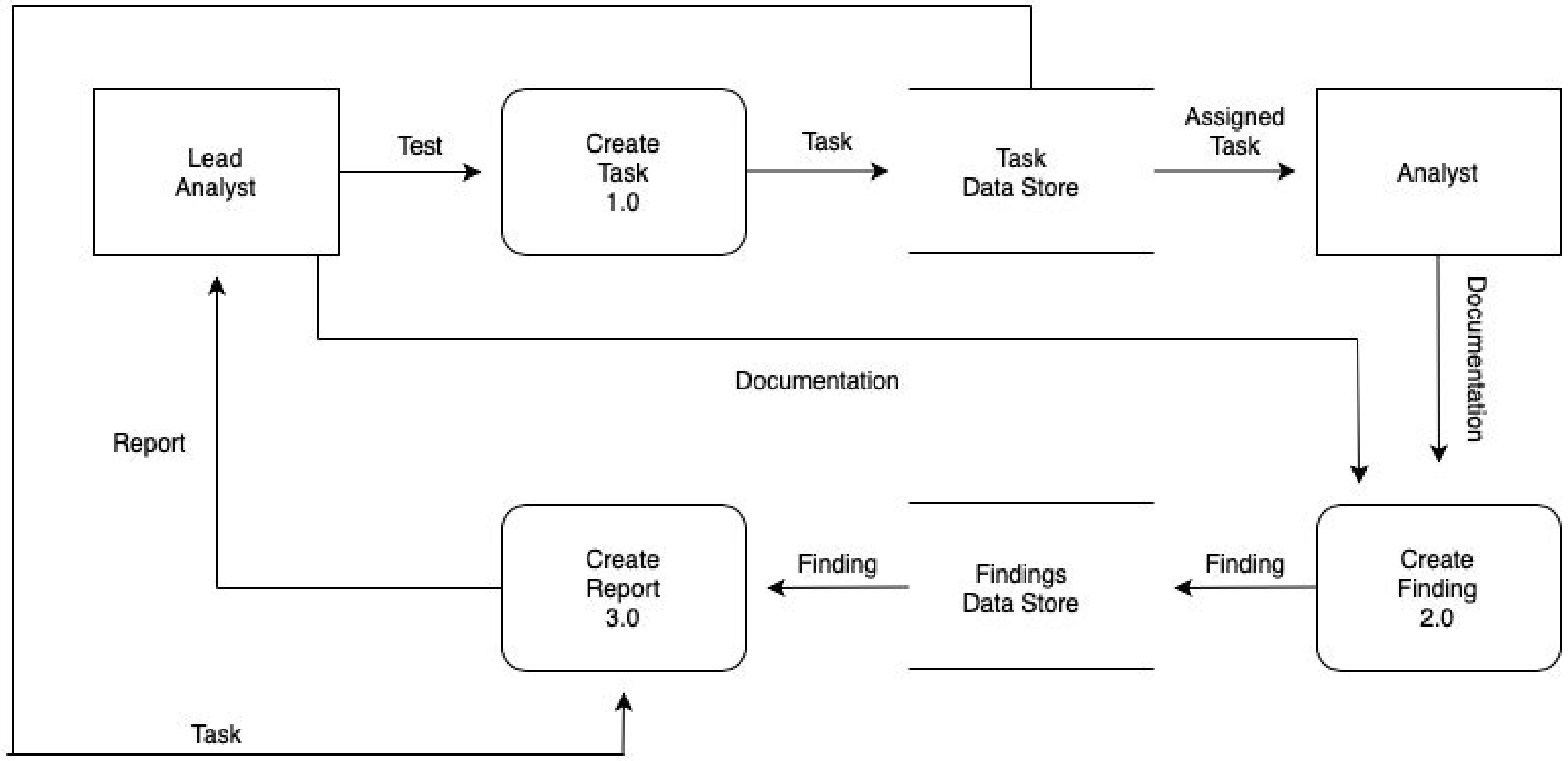
Risk matrix verbs:

- Identify finding type
- Enter description
- Confirm relevance of threat
- Describe mitigation

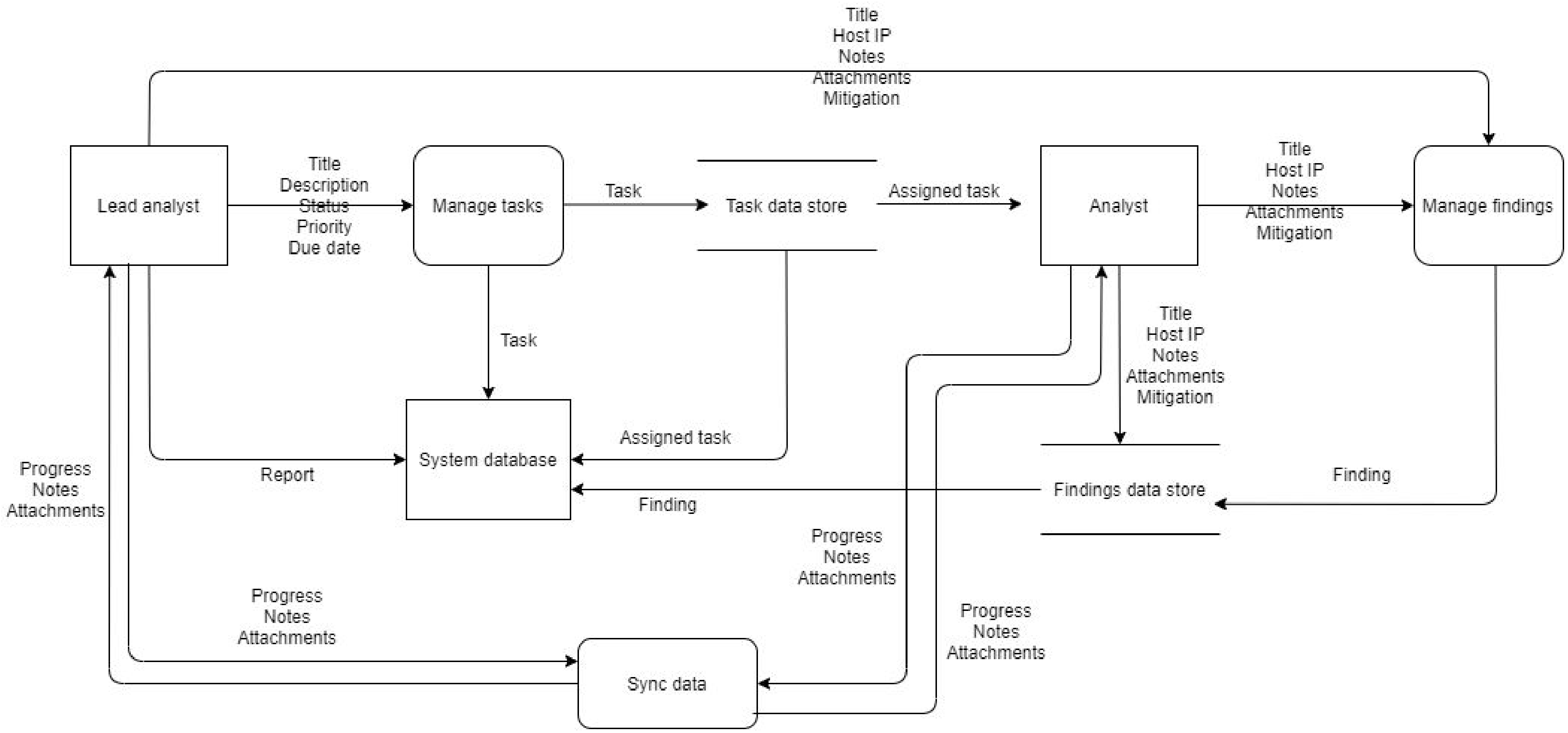
- Alert when task is completed
- Data from old events get saved to hard-drive which hard-drive gets uploaded securely somewhere else

- CM
- Vs (n)
- Vs (q)
- Relevance of threat
- Likelihood
- Impact
- Impact Rationale
- Risk
- Mitigation 1-Liner
- Mitigation
- Analyst

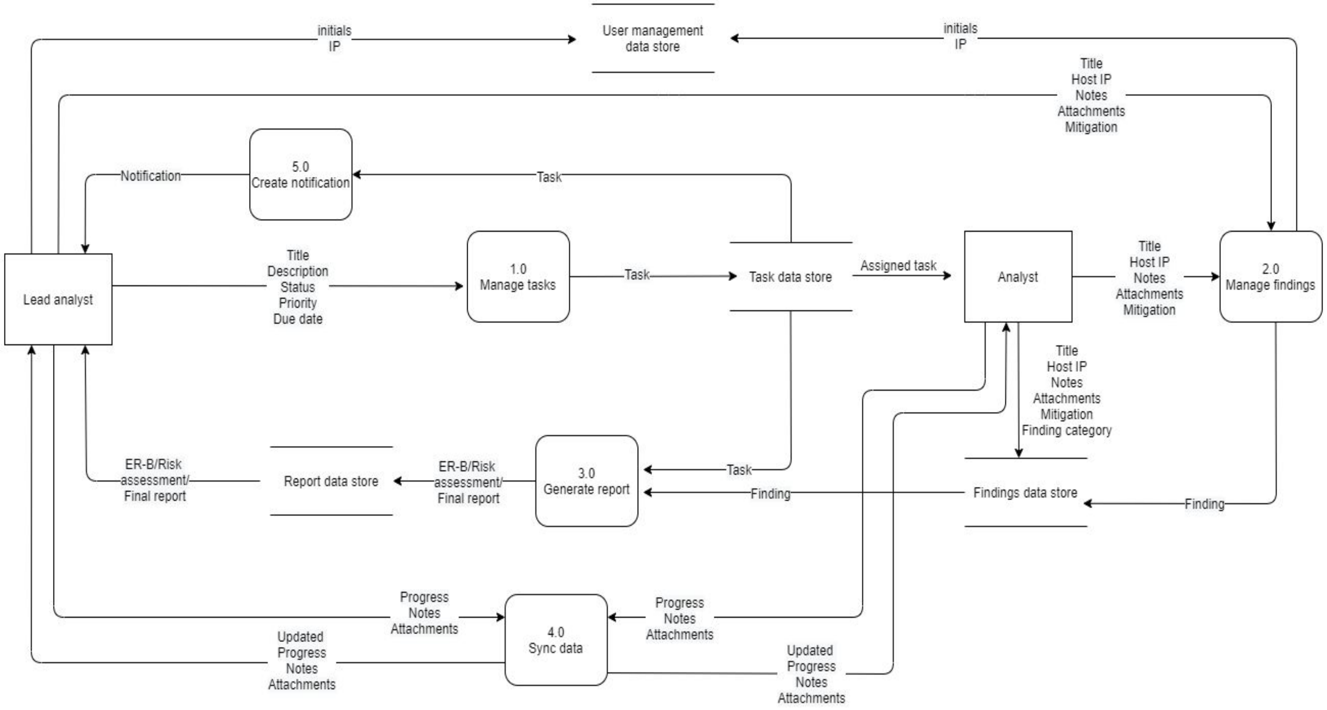
Data Flow Level: Level 1
Version: 1.0.1



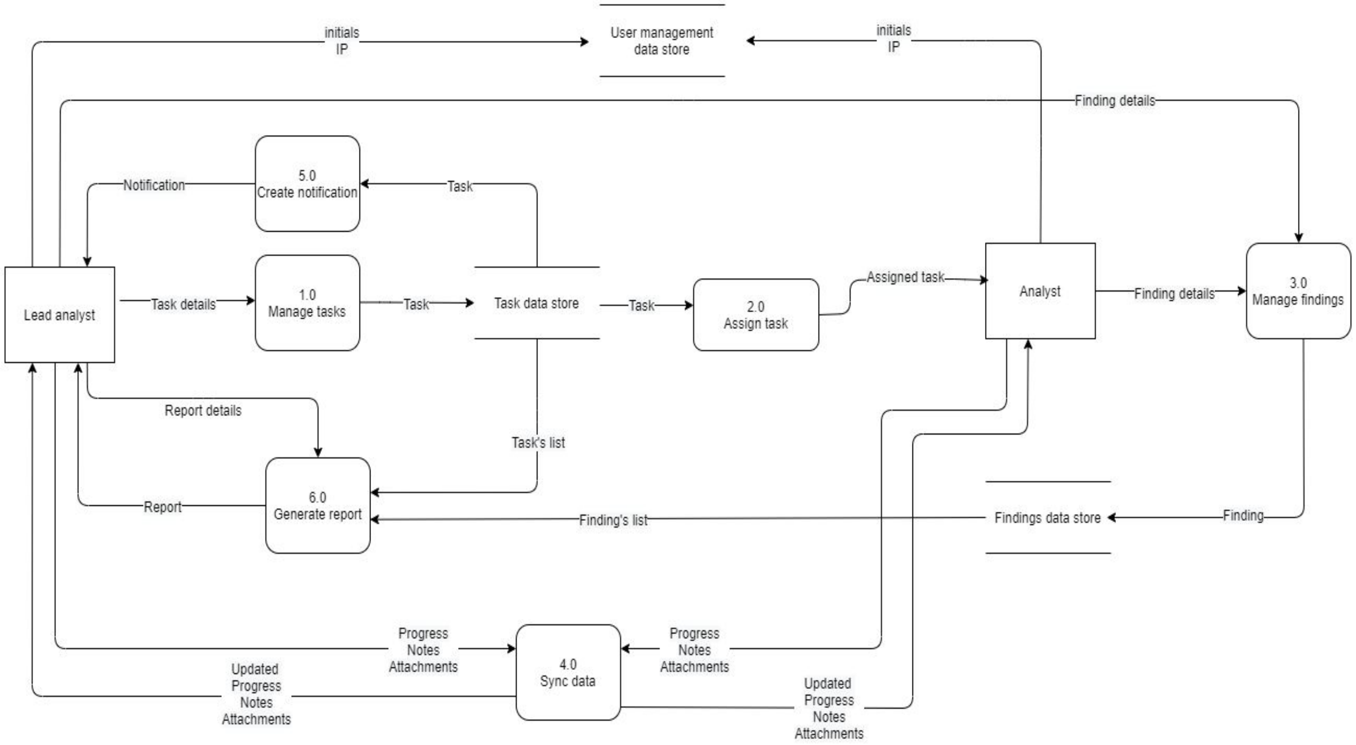
Data Flow Level: Level 1
Version: 1.0.4



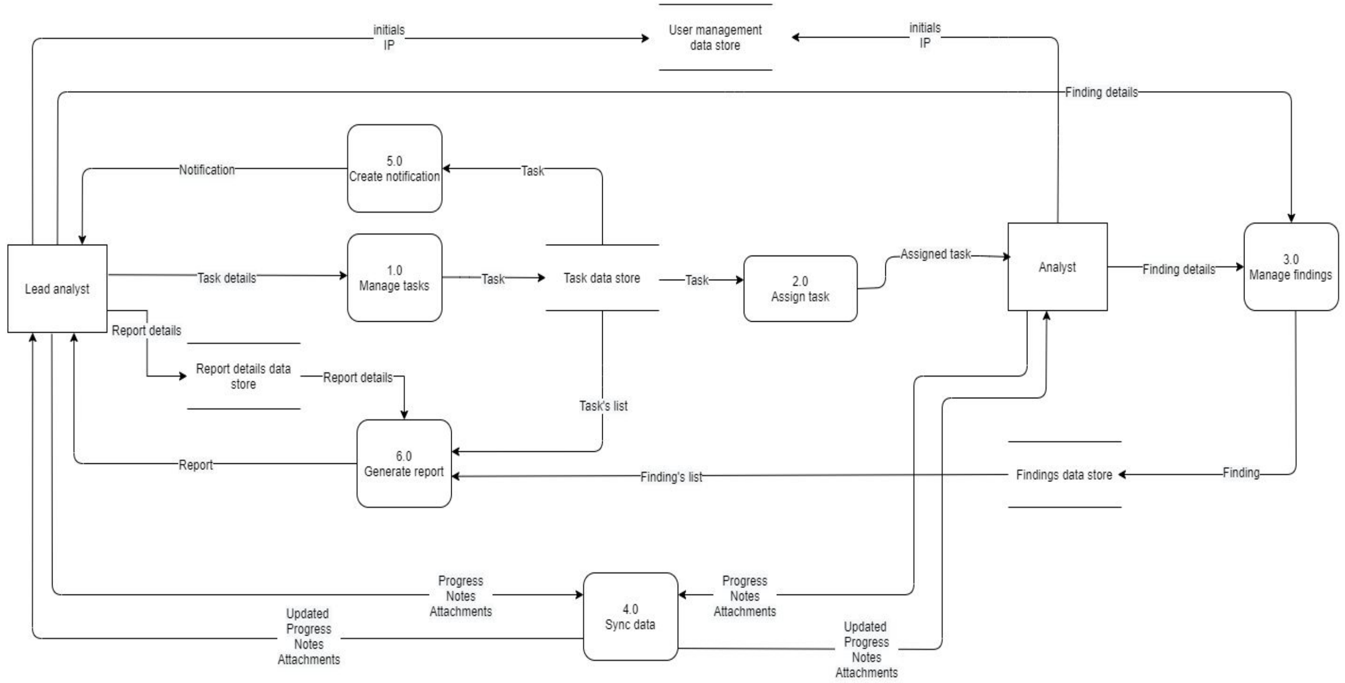
Data Flow Level: Level 1
Version: 1.0.5


User management data store
initials IP
initials IP
Title Host IP Notes Attachments Mitigation
5.0 Create notification
Notification
Task
Lead analyst
Title Description Status Priority Due date
1.0 Manage tasks
Task
Task data store
Assigned task
Analyst
Title Host IP Notes Attachments Mitigation
2.0 Manage findings
Title Host IP Notes Attachments Mitigation Finding category
ER-B/Risk assessment/ Final report
Report data store
ER-B/Risk assessment/ Final report
3.0 Generate report
Task
Finding
Findings data store
Finding
Progress Notes Attachments
4.0 Sync data
Progress Notes Attachments
Updated Progress Notes Attachments
Updated Progress Notes Attachments

Data Flow Level: Level 1
Version: 1.0.8



Data Flow Level: Level 1
Version: 1.0.9

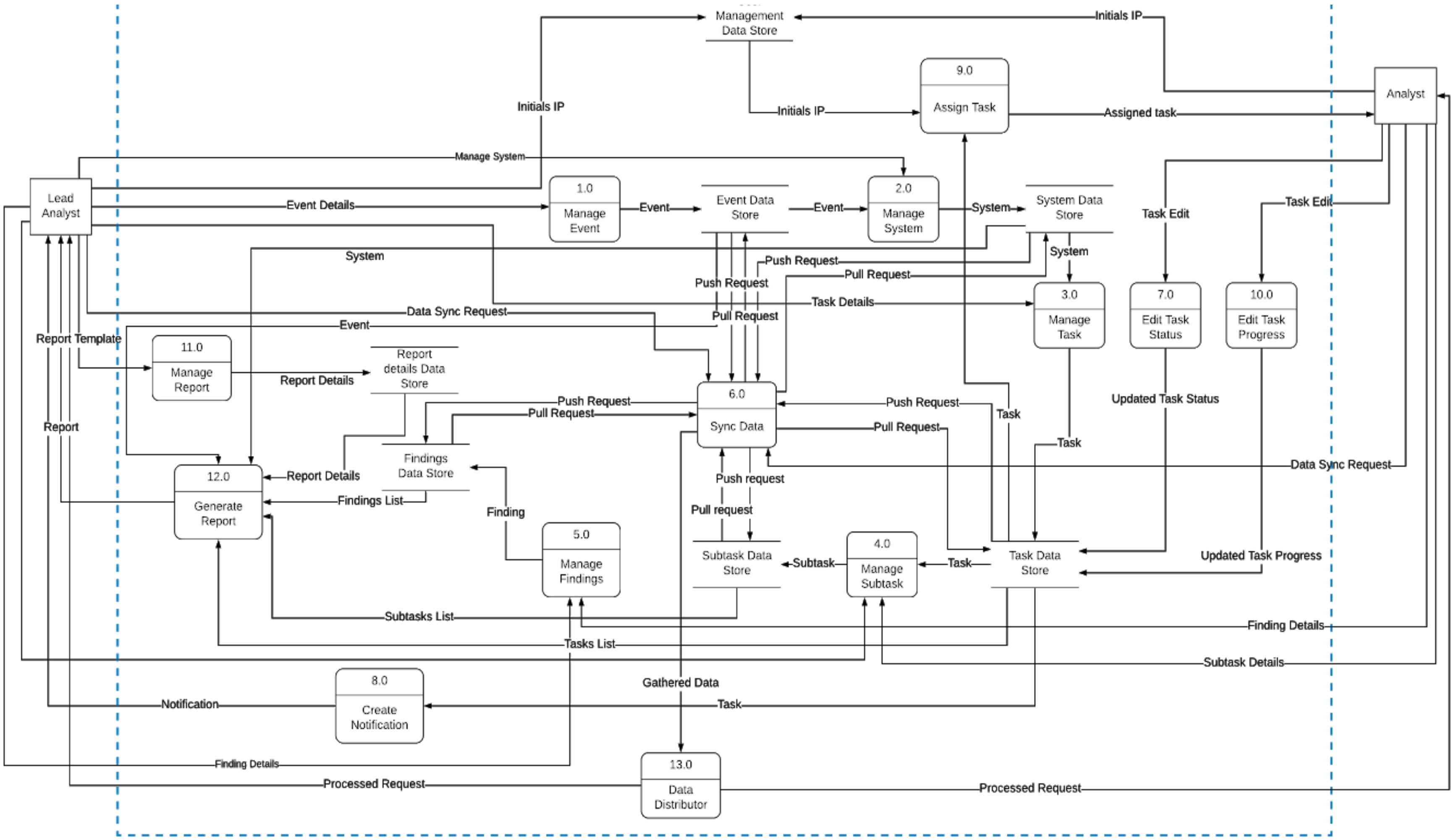


Data dictionary:

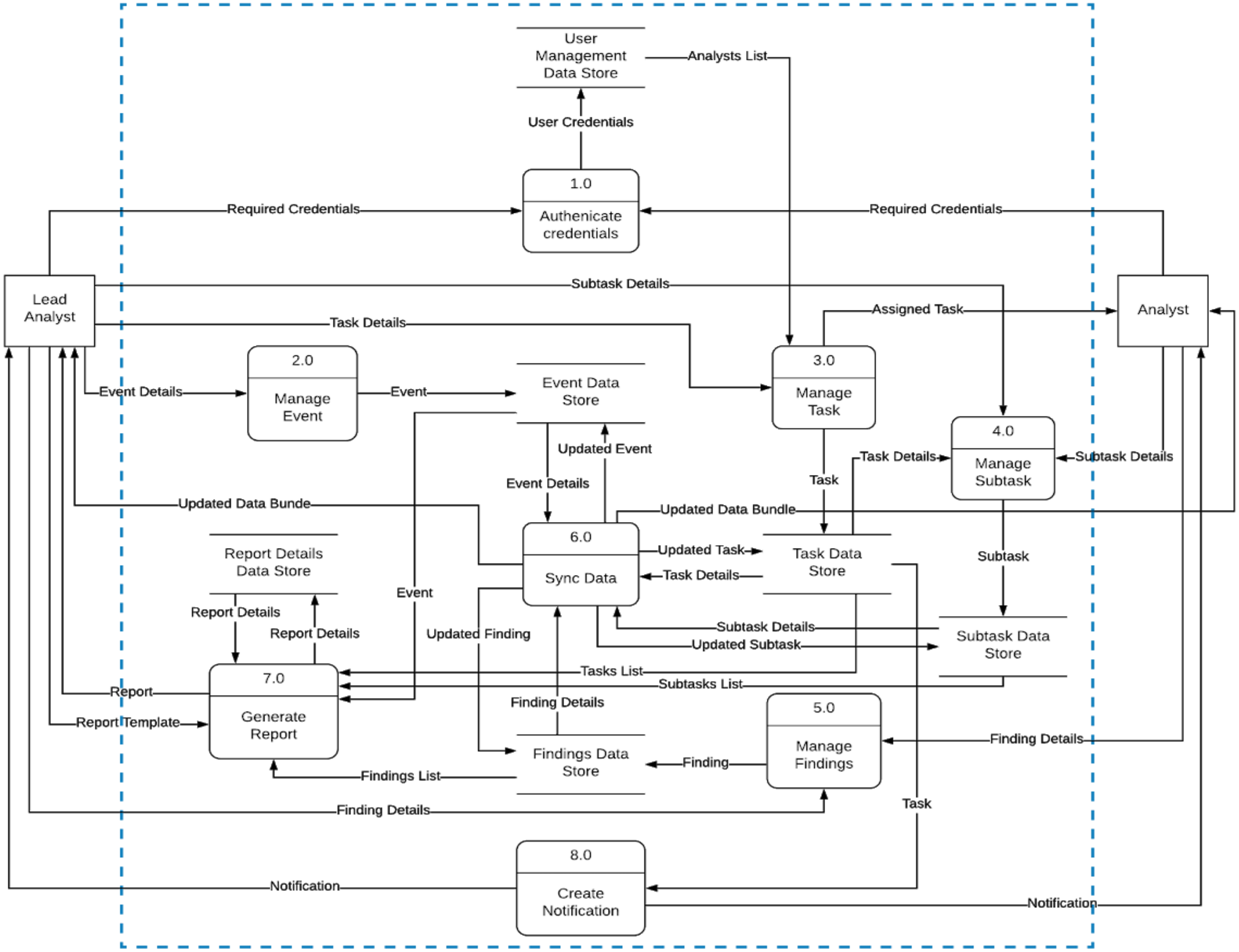
- **Task details:**
    - *Task details refers to a task's title, description, status, priority and due date.*
- **Finding details:**
    - *Finding details refers to a finding's title, hostIP, notes, description, status, likelihood, mitigation, impact, artifacts, evidence, impact, countermeasure and finding type.*
- **Report:**
    - *A report can be an ER-B, risk assessment, or final report.*
- **Report details:**

- *Report details refers not only to the list of findings and tasks for a certain event, but also the following based on a provided risk assessment template:*
    - ***Change log:** contains the changes that have been made to a finding.*
    - ***Overall score card:** contains the risk level, confidentiality, integrity and availability of a finding,*
    - ***Write up cards***
    - ***Tables:** contains tables describing the details of likelihood and relevance of threat.*
    - ***Report template:** provided by the CEAD team.*

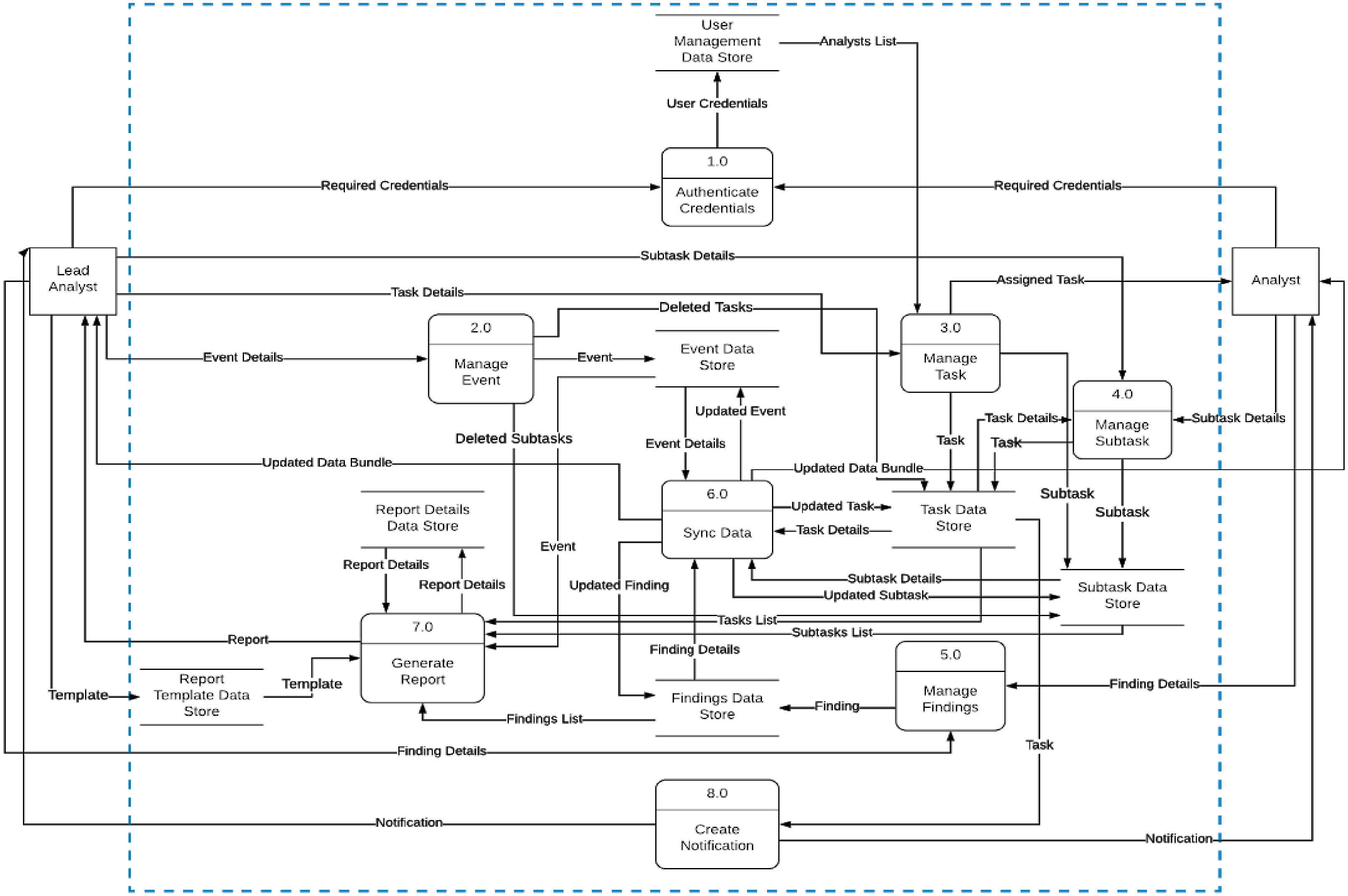
Data Flow Level: Level 1
Version: 1.1.0



Data Flow Level: Level 1
Version: 1.1.1



Data Flow Level: Level 1
Version: 1.1.2

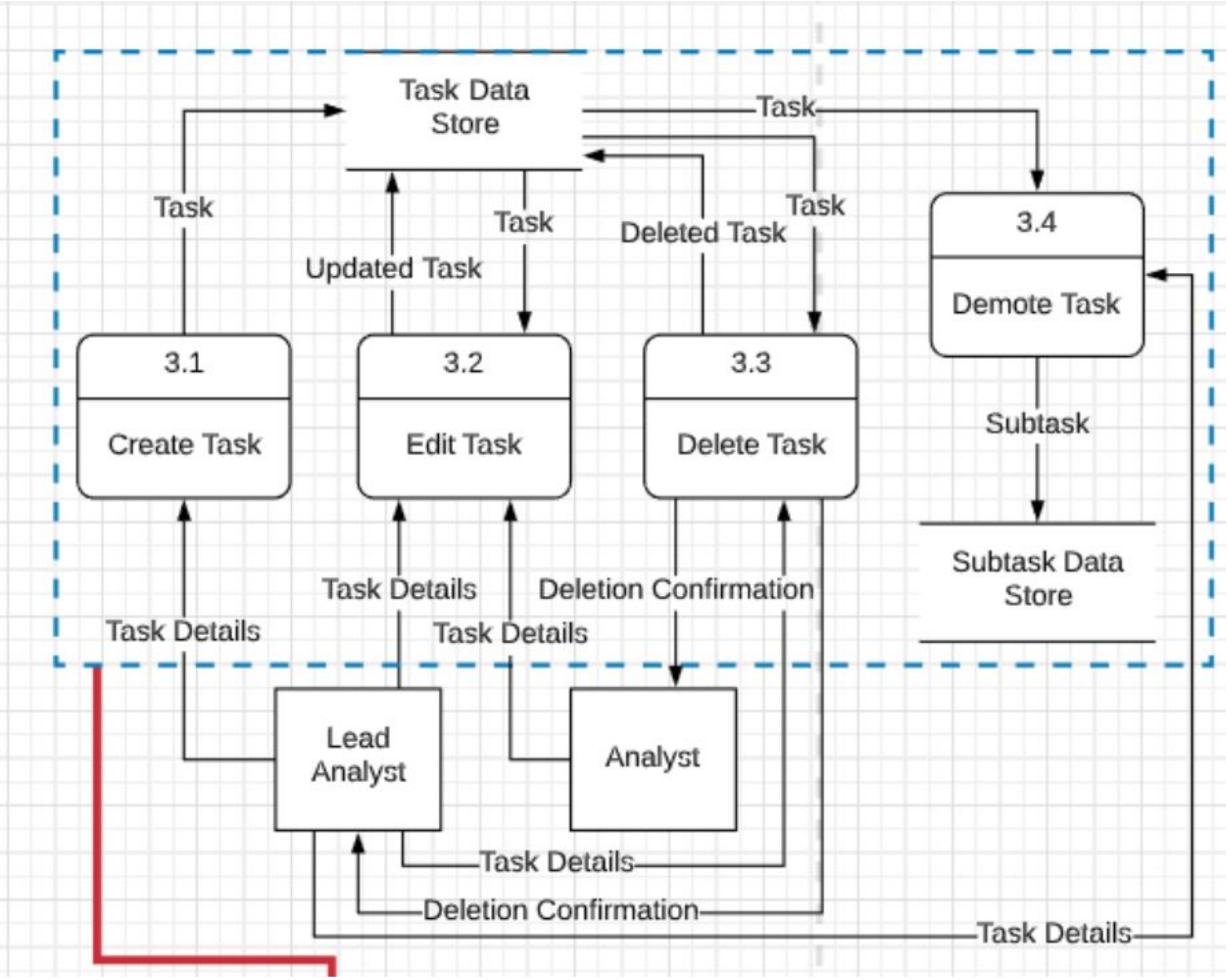


Data dictionary:

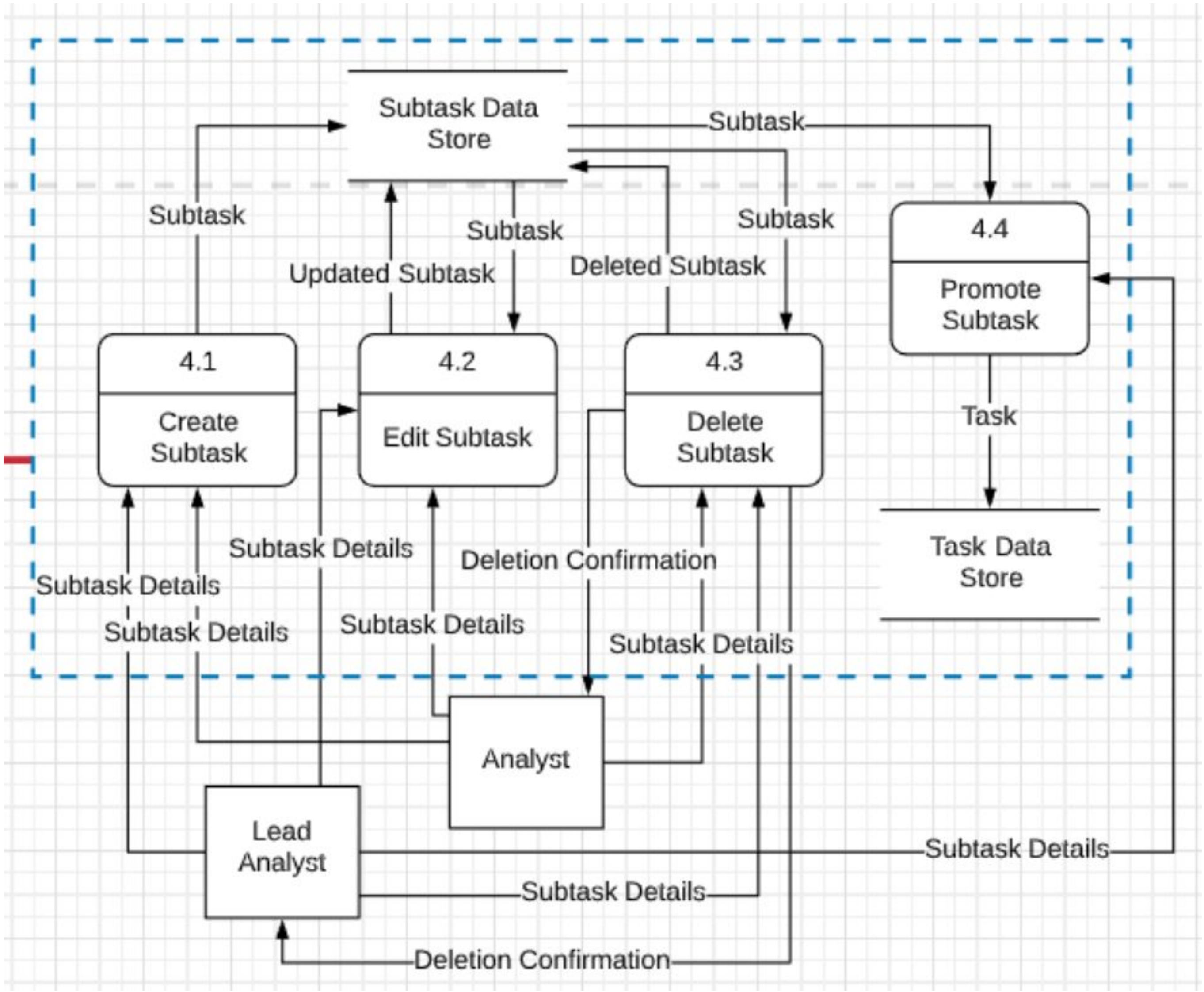
- ***Working assignment:***
    - *Represents any task, subtask, or finding**.***
- ***Working assignment details:***
    - *Working Assignment details refers to the attributes of the corresponding working assignment.*
- ***Event Details:***
    - *Event details refers to the event's tested system, Lead analyst, security classification guide title, declassification, declassification date, organization name, customer name, assessment date, locations, test plan title, switches, routers, access, building accessed, room accessed, event type.*
- ***Task/Subtask's Details:***
    - *Refers to the required task/subtask's attributes in order to create a notification.*
- ***Report:***
    - *A report can be an ER-B, risk assessment, or final report.*
- ***Required Credentials:***
    - *Refers to the analyst's Initials in order to get system access granted.*

Data Flow Level: Level 2
Version: 1.0.0

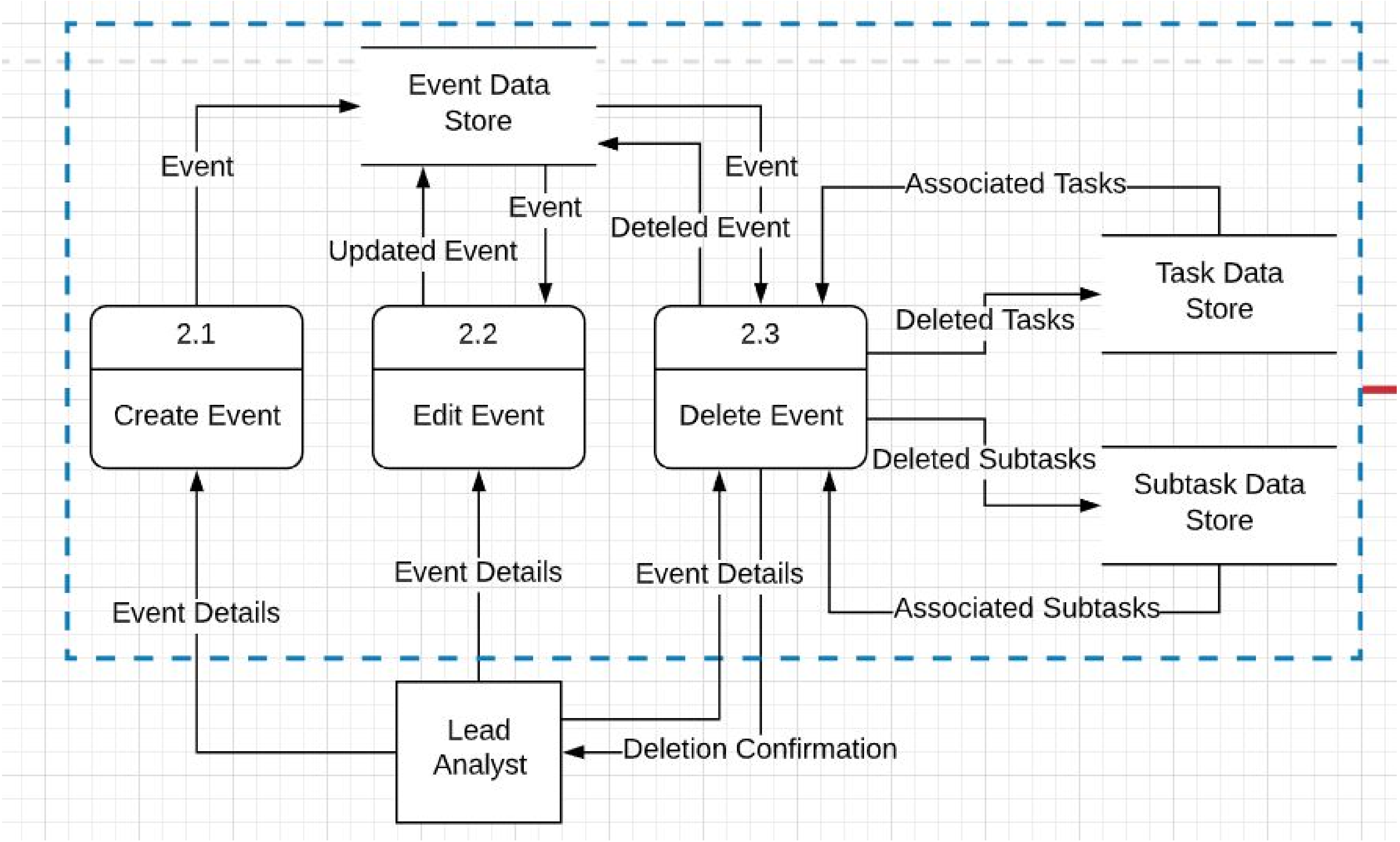
Manage Task:



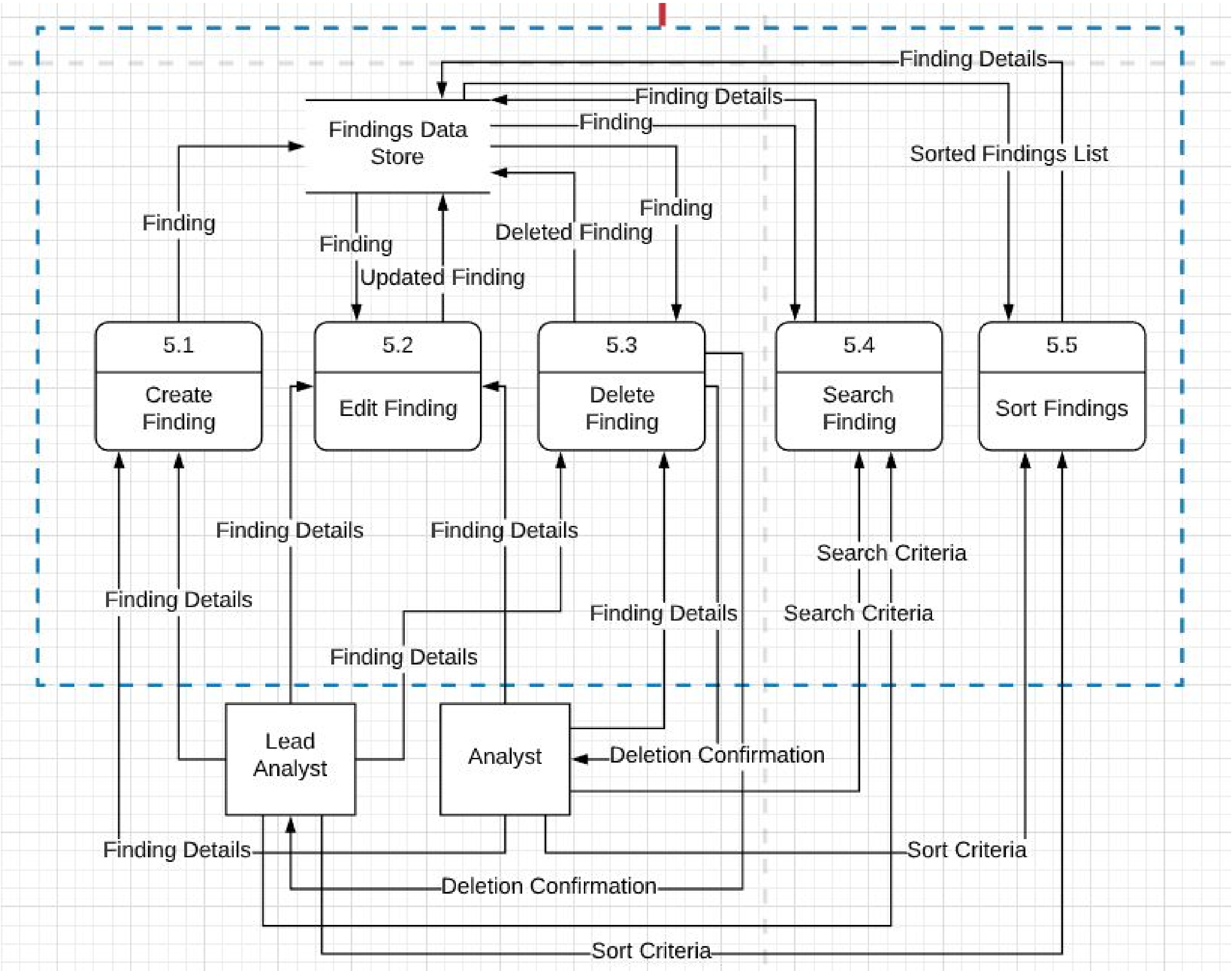
Manage Subtask:



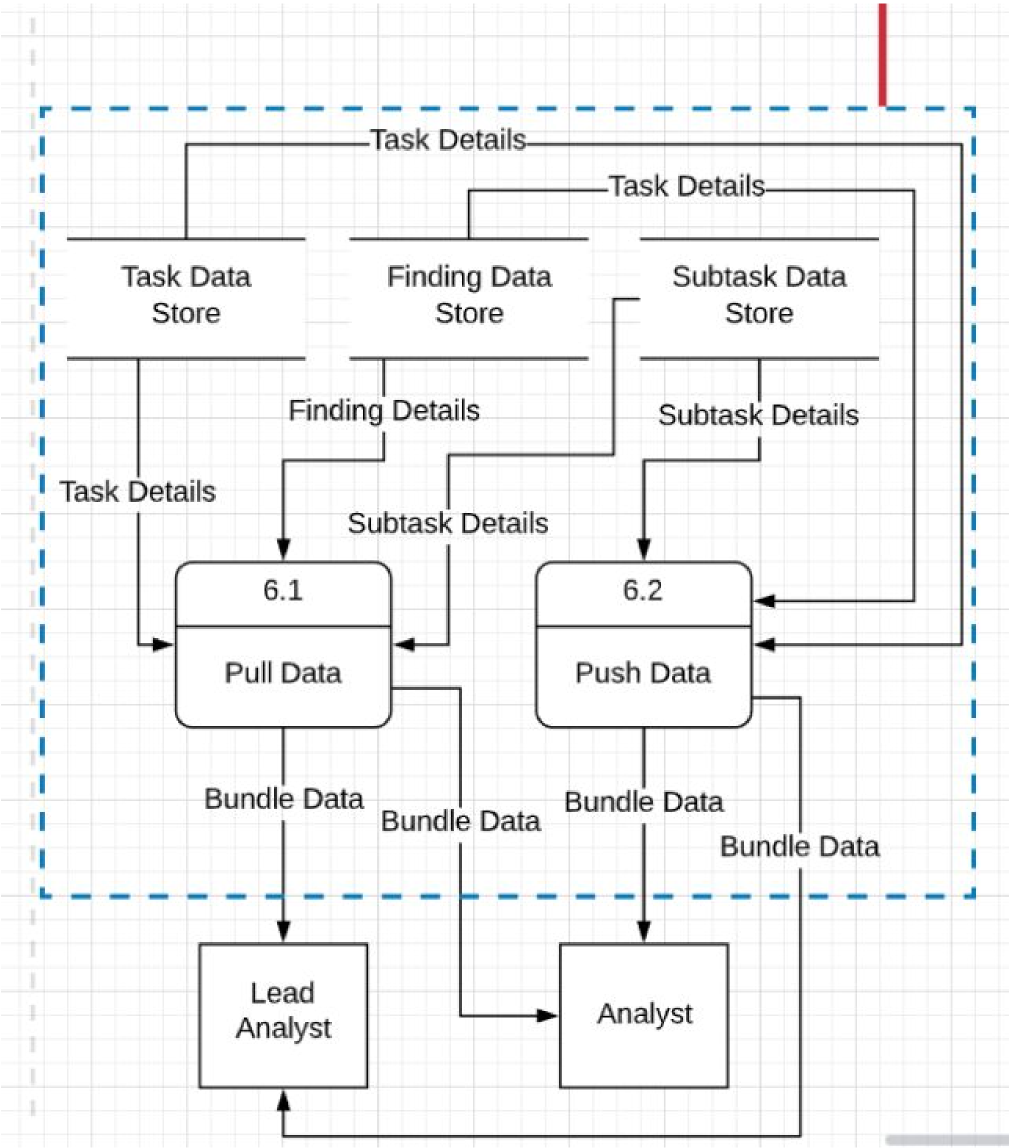
Manage Event:

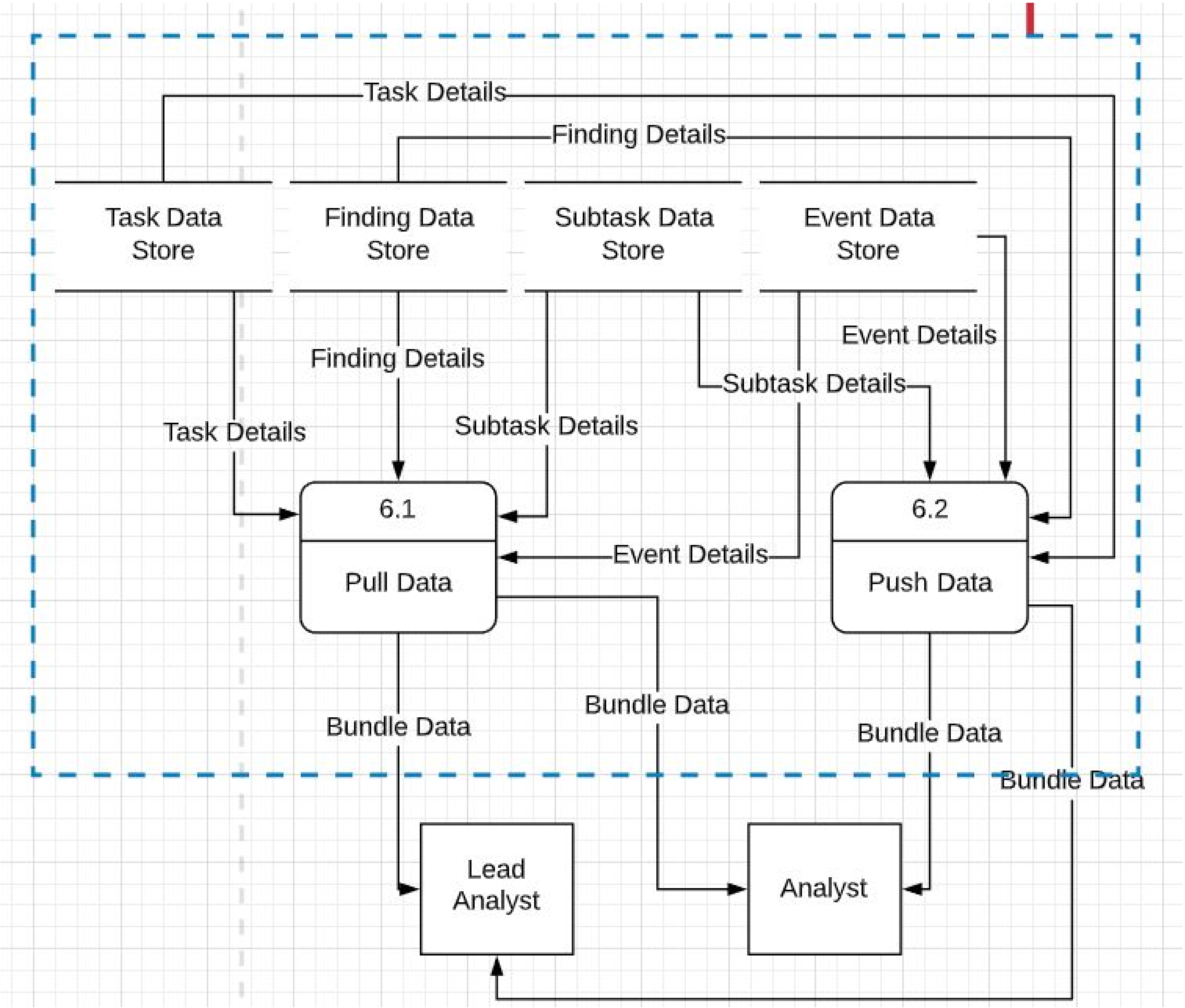


Manage Findings:

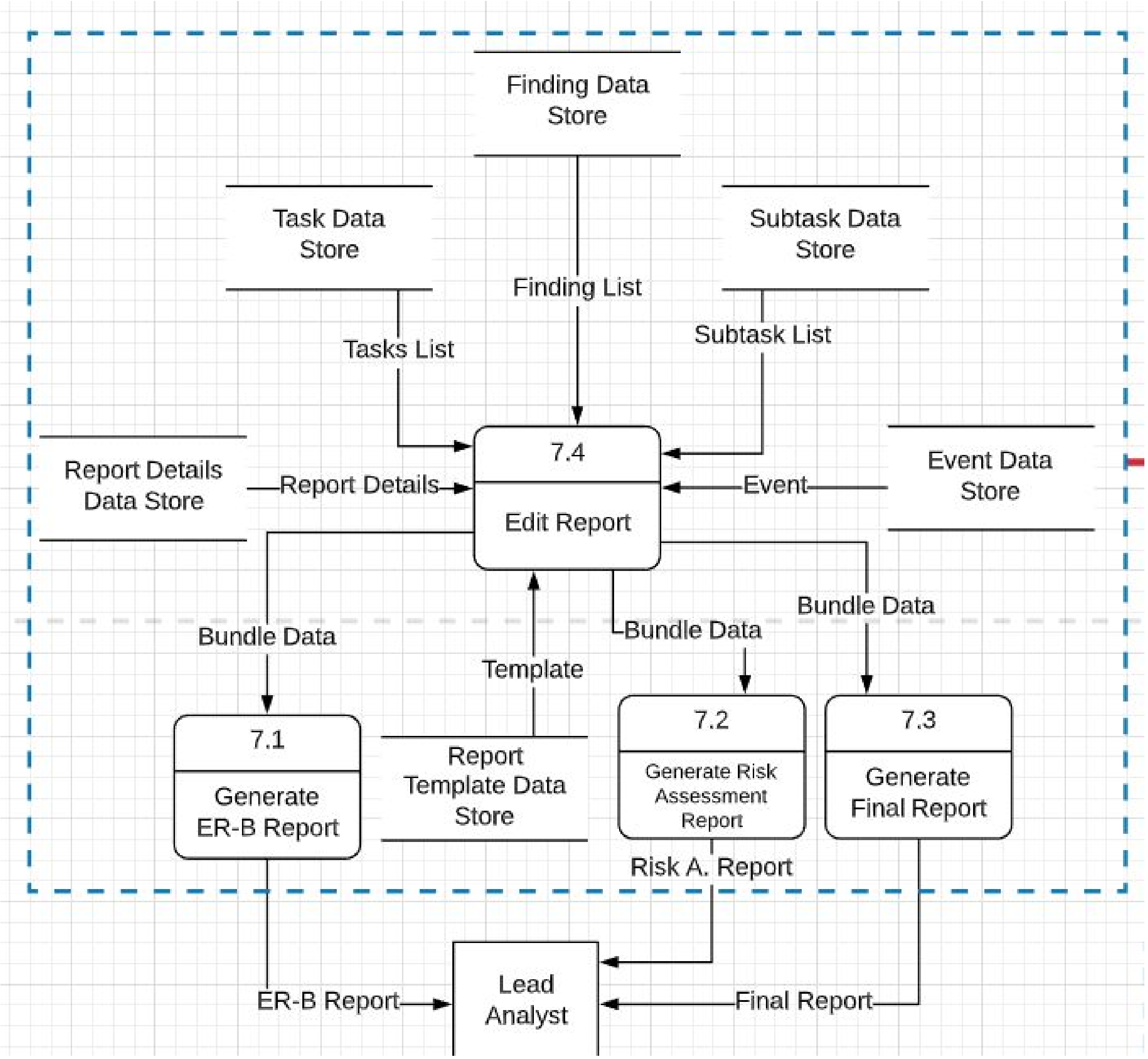


Sync Data:


Task Details
Task Details
Task Data Store
Finding Data Store
Subtask Data Store
Finding Details
Subtask Details
Task Details
Subtask Details
6.1
Pull Data
6.2
Push Data
Bundle Data
Bundle Data
Bundle Data
Bundle Data
Lead Analyst
Analyst

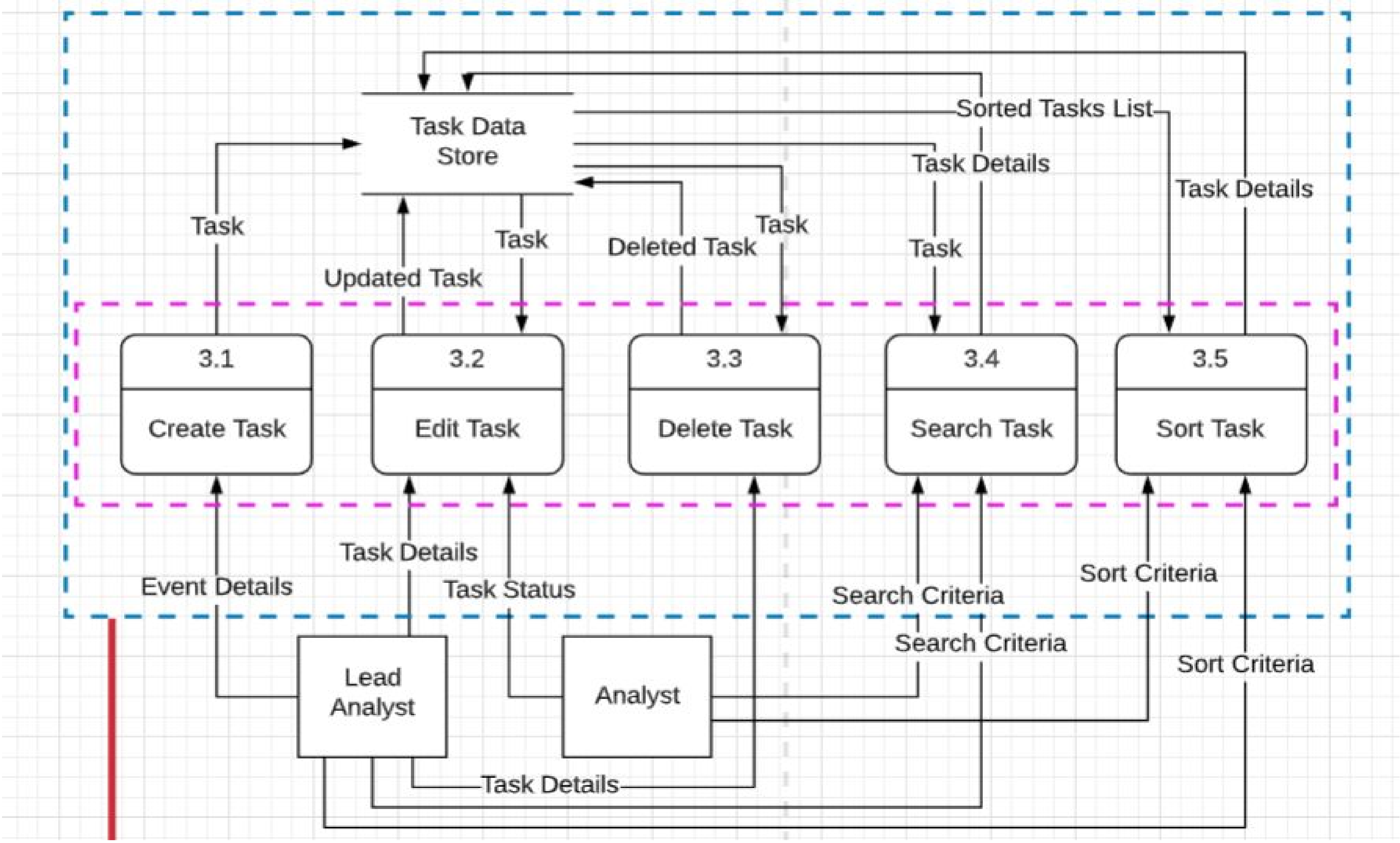

Task Details
Finding Details
Task Data Store
Finding Data Store
Subtask Data Store
Event Data Store
Event Details
Finding Details
Subtask Details
Task Details
Subtask Details
6.1
Pull Data
Event Details
6.2
Push Data
Bundle Data
Bundle Data
Bundle Data
Bundle Data
Lead Analyst
Analyst

Generate Report:



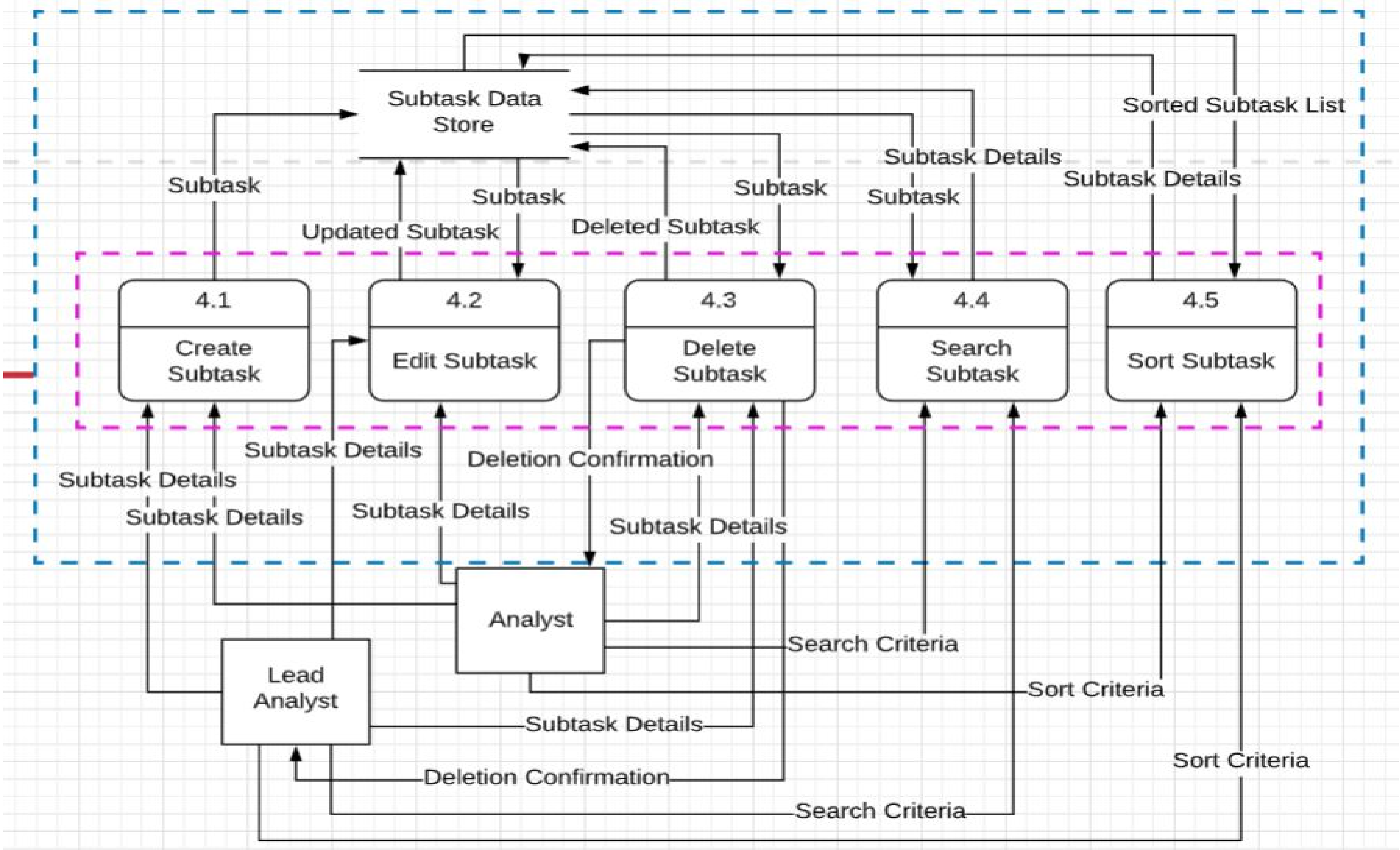
Data Flow Level: Level 2
Version: 1.0.1

Manage Task:



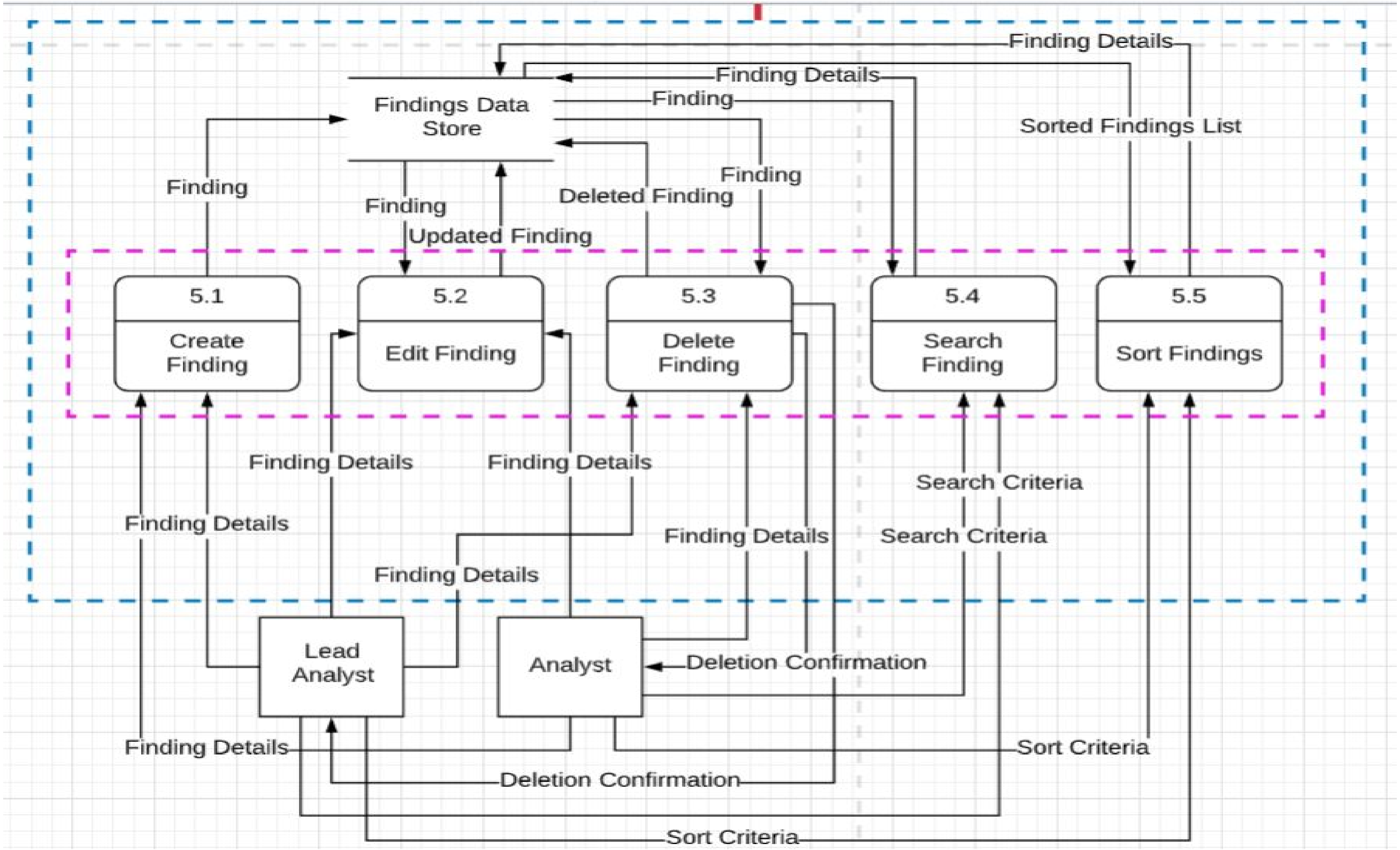
Data Flow Level: Level 2
Version: 1.0.1

Manage Subtask:



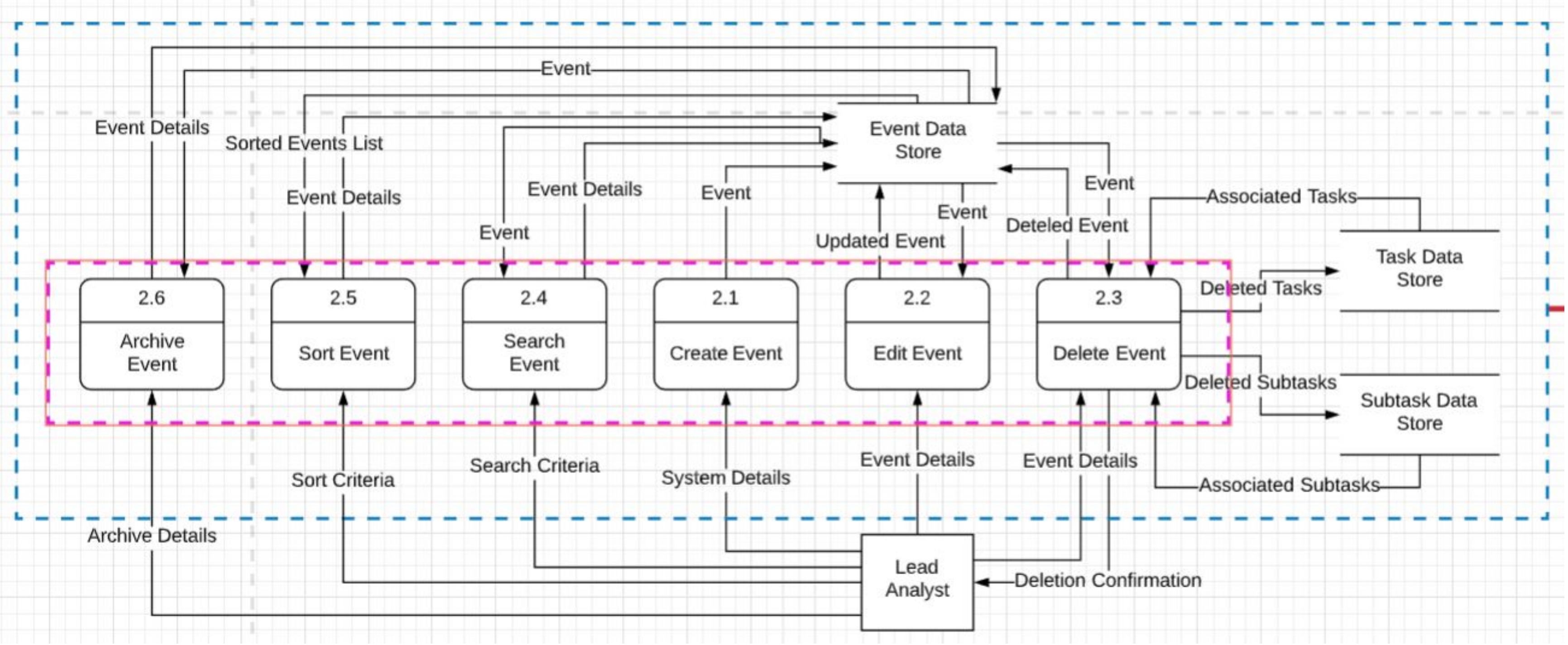
Data Flow Level: Level 2
Version: 1.0.1

Manage Findings:



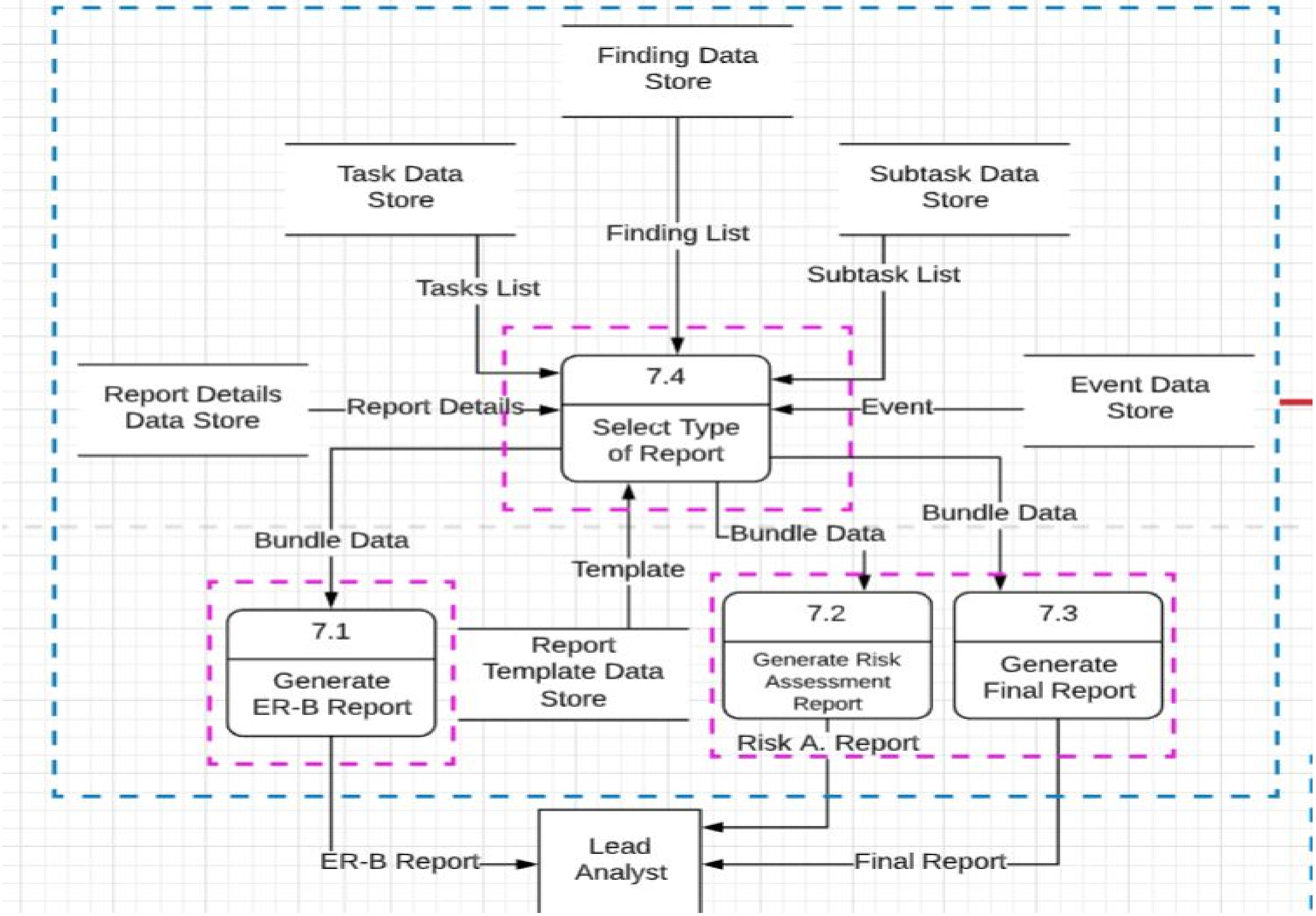
Data Flow Level: Level 2
Version: 1.0.1

Manage Events:

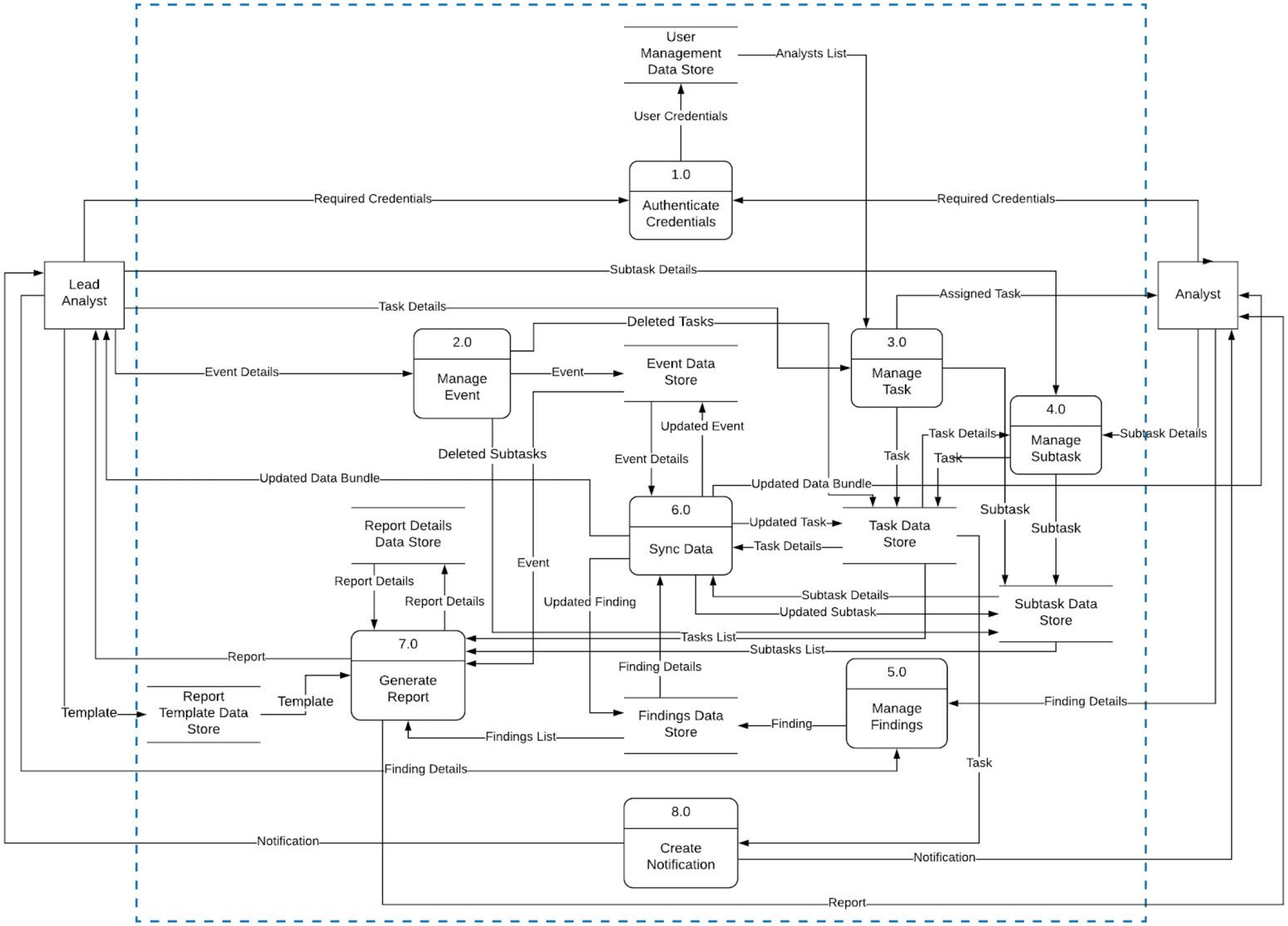


Data Flow Level: Level 2
Version: 1.0.1

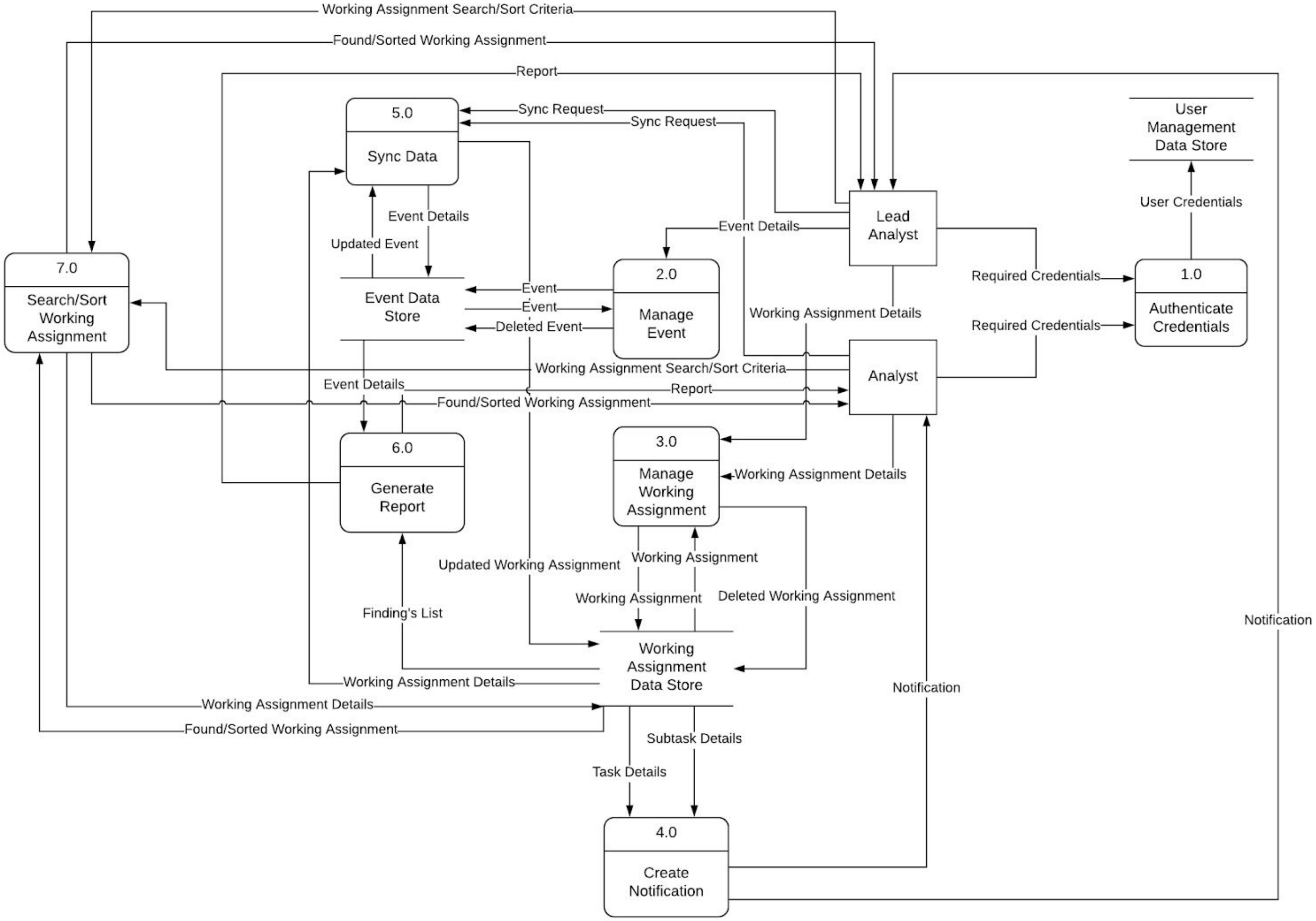
Generate Report:



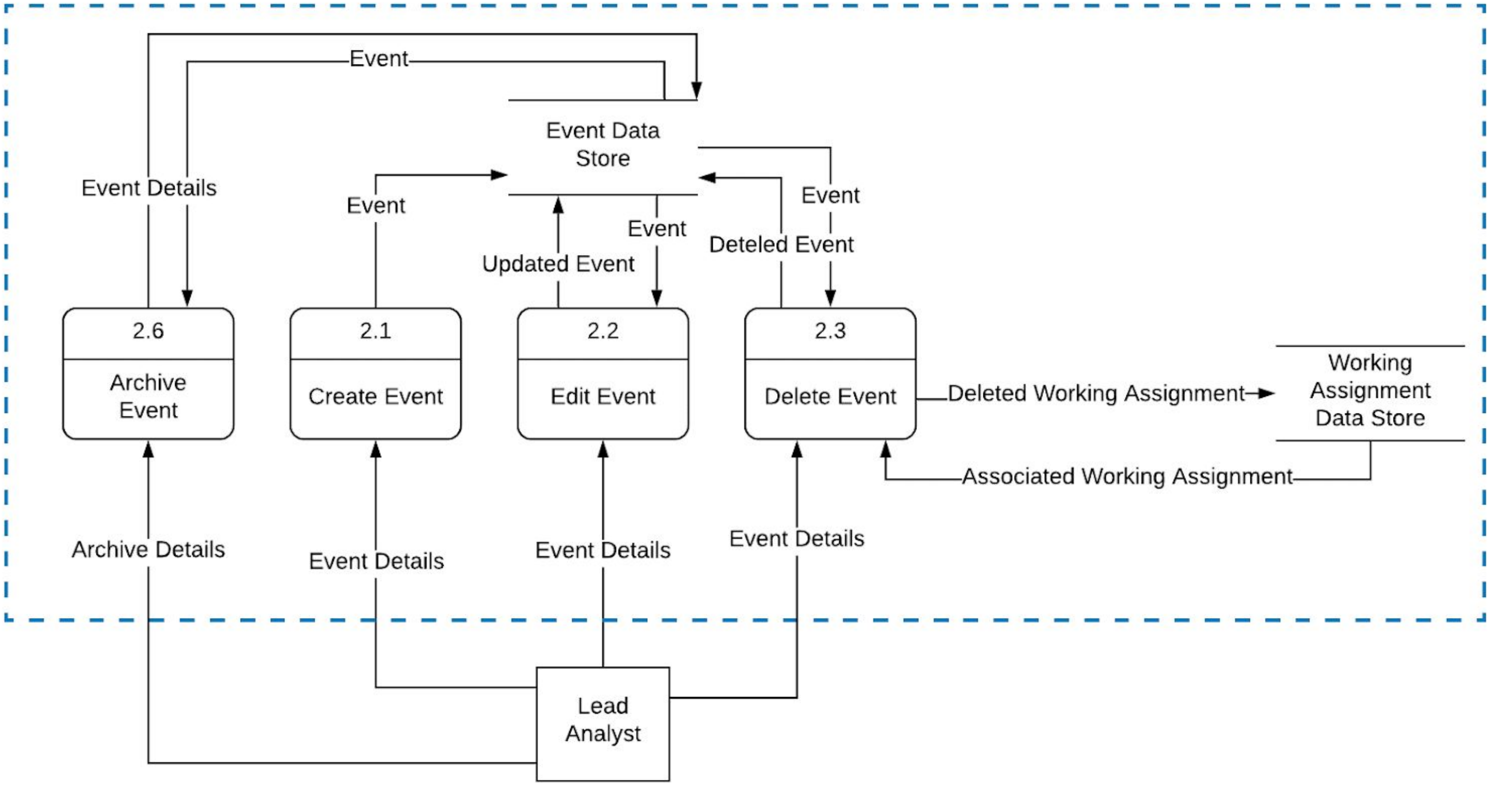
Data Flow Level: Level 1
Version: 1.1.3



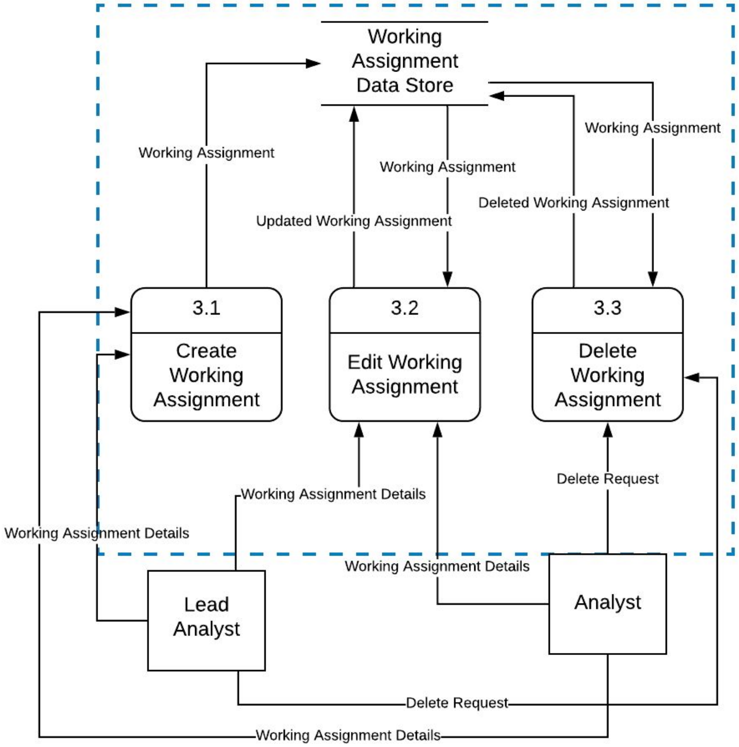
Data Flow level: 1
Version: 1.1.4


Working Assignment Search/Sort Criteria
Found/Sorted Working Assignment
Report
Sync Request
Sync Request
5.0
Sync Data
User Management Data Store
User Credentials
Event Details
Updated Event
Event Details
Lead Analyst
7.0
Search/Sort Working Assignment
2.0
Manage Event
Required Credentials
1.0
Authenticate Credentials
Event Data Store
Event
Event
Deleted Event
Working Assignment Details
Required Credentials
Analyst
Working Assignment Search/Sort Criteria
Event Details
Report
Found/Sorted Working Assignment
6.0
Generate Report
3.0
Manage Working Assignment
Working Assignment Details
Updated Working Assignment
Working Assignment
Working Assignment
Deleted Working Assignment
Finding's List
Notification
Working Assignment Data Store
Working Assignment Details
Working Assignment Details
Found/Sorted Working Assignment
Notification
Subtask Details
Task Details
4.0
Create Notification

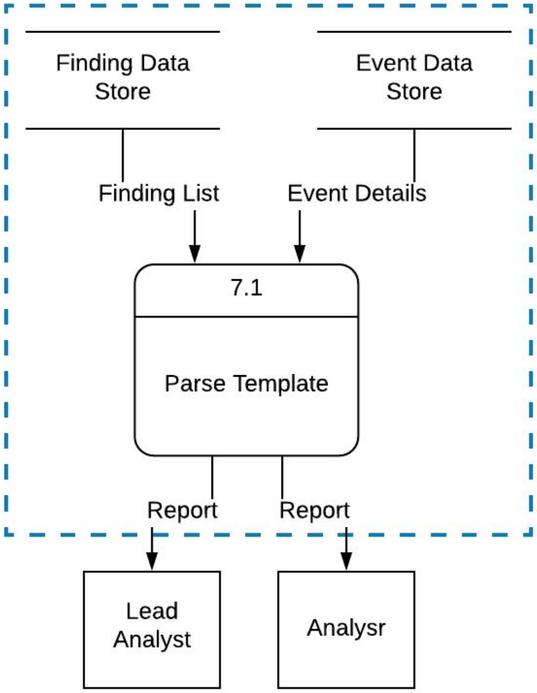
Data flow level: 2
Version 1.1.4



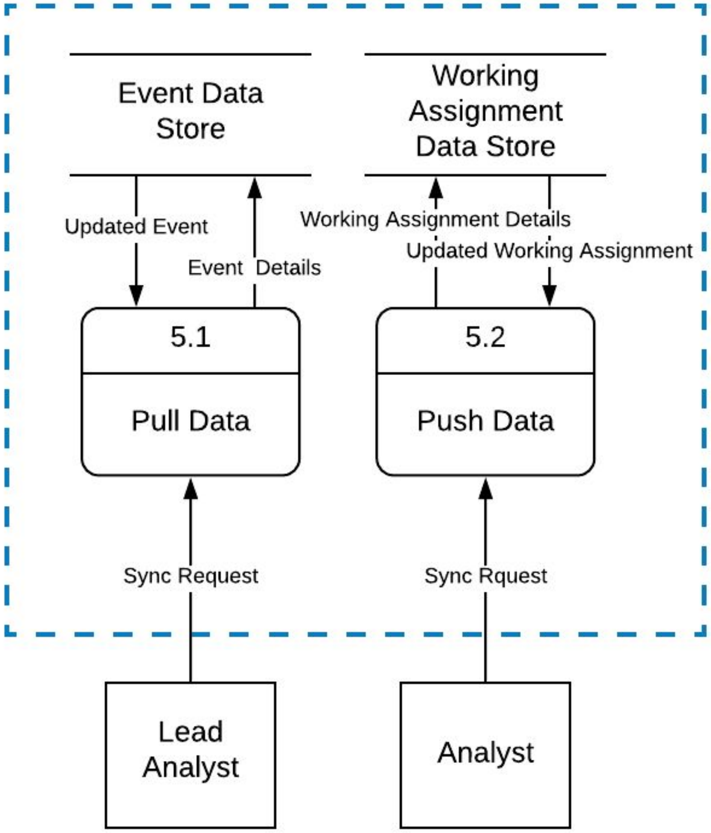
Manage Event


Working Assignment Data Store
Working Assignment
Working Assignment
Updated Working Assignment
Deleted Working Assignment
Working Assignment
3.1
Create Working Assignment
3.2
Edit Working Assignment
3.3
Delete Working Assignment
Working Assignment Details
Delete Request
Working Assignment Details
Working Assignment Details
Lead Analyst
Analyst
Delete Request
Working Assignment Details

Manage Working Assignment



Generate Report


Event Data Store
Working Assignment Data Store
Updated Event
Event Details
Working Assignment Details
Updated Working Assignment
5.1
Pull Data
5.2
Push Data
Sync Request
Sync Rquest
Lead Analyst
Analyst

Sync Data