



# Layer 4: Data Agnostic Specification

**Purpose:** To focus on high-level, data agnostic requirements that enable interoperable, modularized CM components that can be used to compose CM-based systems with minimal to no integration cost.

- Based on the CAESARS FE Use Cases
- Defines requirements for each interface in the CAESARS FE model
  - Communications Protocols and Models (e.g. HTTP/HTTPS, Java Message Service, Advanced Message Queuing Protocol, etc.)
  - Messaging Protocols and Models (e.g. SOAP, RestMS, etc.)
  - Communications Models (e.g. Asset Reporting Format (ARF), etc.)
  - Additional interface requirements to enable the CAESARS FE Use Cases
    - Tracking identifiers
    - High-level, generalized processing requirements

# Layer 4: Data Agnostic Specification (cont.)

Discussion points for each interface

- What are the appropriate communications protocol(s) to standardize around for each interface?
- What messaging protocols make the most sense for each interface?
- What existing specifications and standards can we leverage to model communications?
- What additional requirements do we need to define for each interface to support interoperability?
  - Are there additional communications parameters we need to capture?
  - Are there high-level, generalized processing requirements that are important for interoperability?

# **INTRA-INSTANCE INTERFACES**

# Interface I1

**Purpose:** Provides requested data for scoring and presentation.

**Provider:** Common Interface over: Repository of Findings, Metrics Repository and Asset Inventory

**Clients:** Analysis / Scoring (Scoring Engine), Task Manager (Query Orchestrator)

**Example Data:** Assessment Summary Results

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

**Request Model:** TBD

**Response Model:** ARF Based

## Notes:

- Must be able to provide metadata relating to the freshness of available data.
- Must be able to retrieve requested data and trigger data collection if the requested data is not available or does not meet the freshness requirements.

# Interface I2

**Purpose:** Provides queried data for presentation.

**Provider:** Task Manager (Query Orchestrator)

**Clients:** Presentation / Reporting (Dashboard Engine),  
Task Manager (Inter-Tier Reporting)

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

**Request Model:** TBD

**Response Model:** ARF Based

# Interface I4

**Purpose:** To retrieve content used for data collection and to provide context for analysis

**Provider:** Content Subsystem

**Clients:** Collection Subsystem, Analysis / Scoring Subsystem

**Example Data:** SCAP Content, Digital Event Collection Rules, Remediation Data, Organizational Policies

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

# Interface I5

**Purpose:** Enable the orchestration of queries and tasking for report generation within and between CM instances.

**Provider:** Task Manager (Query Orchestrator)

**Clients:** Task Manager (Inter-Tier Reporting)

**Example Data:** Predefined views, Reporting Queries

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

**Request Model:** TBD

**Response Model:** ARF Based

# Interface I7

**Purpose:** Provides de-conflicted data for scoring and presentation.

**Provider:** Analysis / Scoring (Data De-Confliction)

**Clients:** Analysis / Scoring (Scoring Engine)

**Example Data:** Assessment Summary Results,  
Checklist results

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

**Request Model:** TBD

**Response Model:** ARF Based

# Interface I8

**Purpose:** To deposit data into the repository of findings and/or asset inventory.

**Provider:** Data Aggregation (Repository of Findings and Asset Inventory)

**Clients:** Collection Subsystem

**Example Data:** SCAP Results, Event Data

**Transmission Synchronization:** Asynchronous

**Messaging Pattern:** Publish/Subscribe

**Message Model:** ARF Based

## Notes:

- Note that this interface supports both asset inventory collection subsystems and security-focused collection subsystems.
- Might be the same as I9

# Interface I9

**Purpose:** To deposit data into the metrics repository after scoring

**Provider:** Data Aggregation (Metrics Repository)

**Clients:** Analysis / Scoring (Scoring Engine)

**Example Data:** Assessment Summary Results

**Transmission Synchronization:** Asynchronous

**Messaging Pattern:** Publish/Subscribe

**Message Model:** ARF Based

## Notes:

- Might be the same as I8

# **MULTI-INSTANCE INTERFACES**

# Interface I12

**Purpose:** Enable the orchestration and exchange of information based on predefined views and dynamic queries between CM instances.

**Provider:** Task Manager (Inter-Tier Reporting) at a lower tier

**Clients:** Task Manager (Inter-Tier Reporting) at a higher tier

**Example Data:** Predefined views, Reporting Queries

**Transmission Synchronization:** Synchronous

**Messaging Pattern:** Request/Response

**Request Model:** TBD

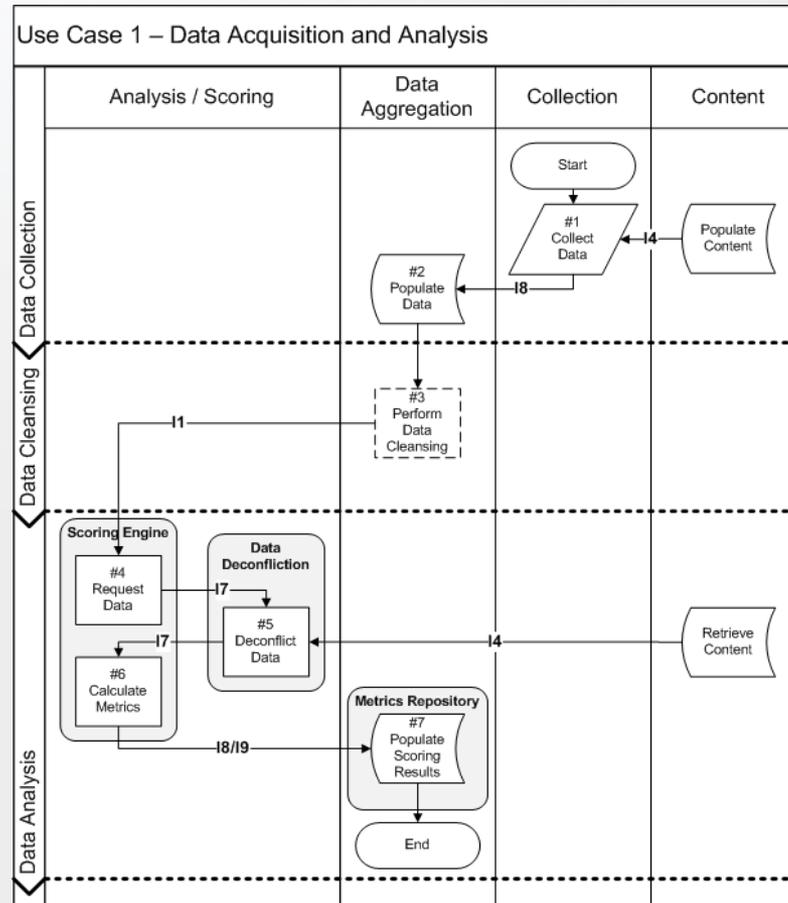
**Response Model:** ARF Based

## Notes:

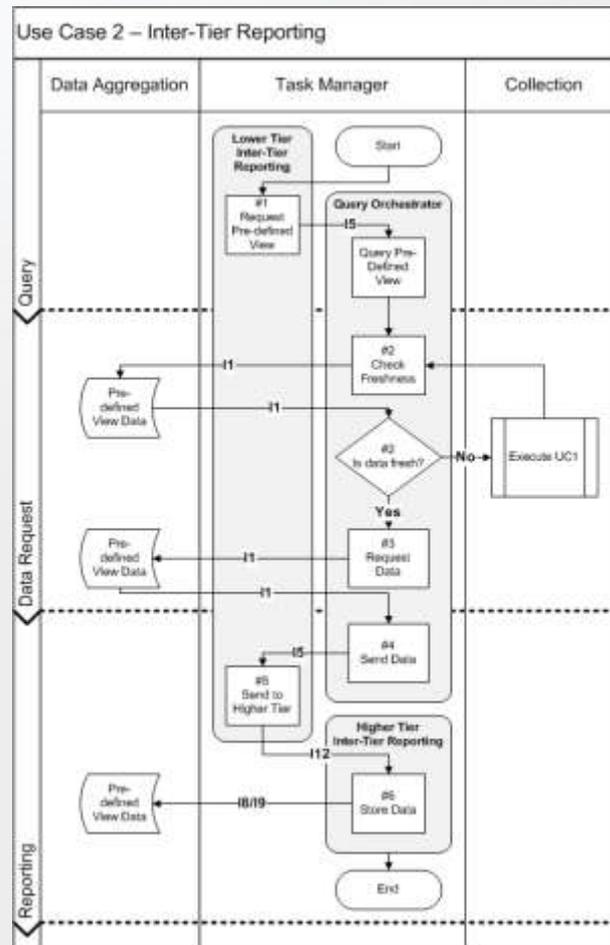
- This data is typically aggregate statistics or compliance data.

**BACKUP SLIDES**

# Use Case 1 – Data Acquisition and Analysis



# Use Case 2 – Inter-Tier Reporting



# Use Case 3 – Intra-Instance Query

