RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PDAC-R03

Context-Based Data Sensitivity Classification

Anchit Arora
Program Manager
Cisco
@ancarora

John Cashman
Information Security Architect
Cisco
@jdcashman

Where's my Data?

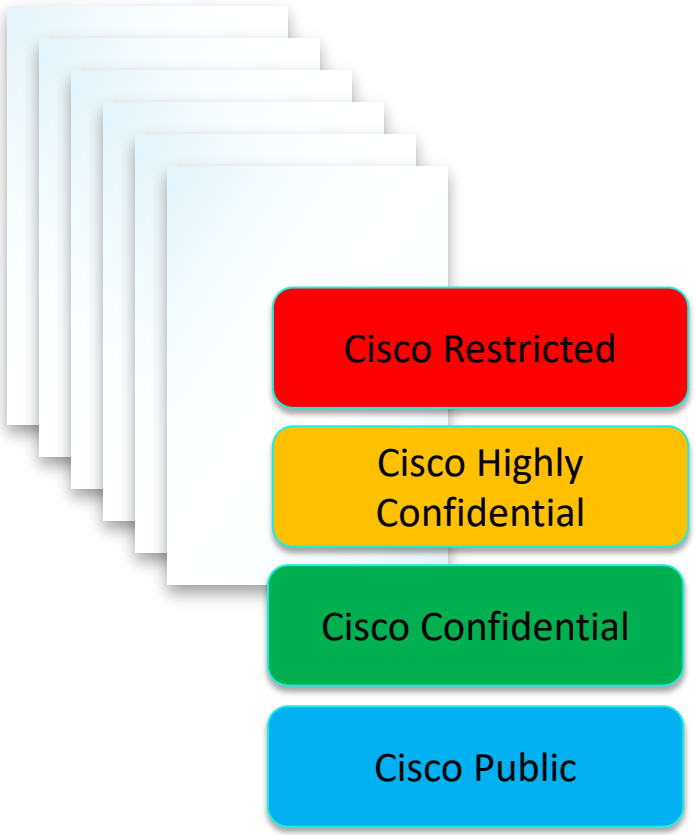
80% of enterprise companies don't know where their sensitive data is located [1]

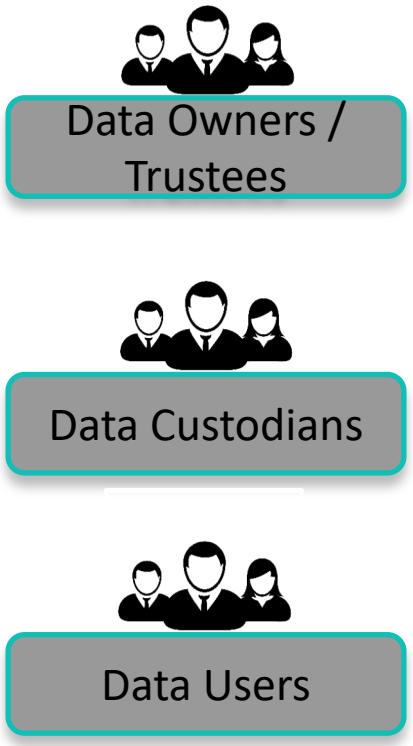
[1] https://thycotic.com/resources/cybersecurity-metrics-report-2017/

Questions that need to be answered to protect data efficiently and effectively

- What is this data?
- What is the source of the data?
- What is the sensitivity of the data?
- Who owns or is accountable for this data?
- *What, if anything, about the form or usage of this data would alter its sensitivity?*

Cisco's Data Classification Framework





Data Classification Adoption Challenge

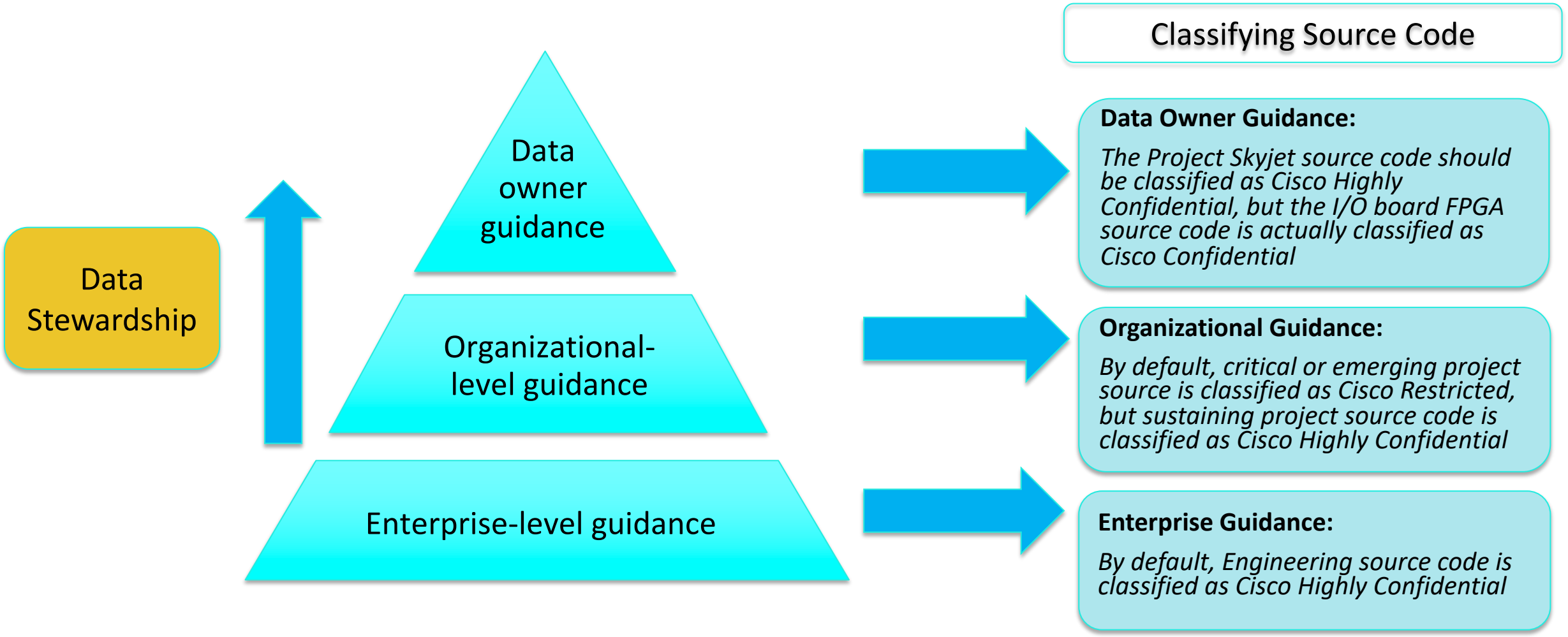
Data Stewardship

Data owner guidance

Organizational-level guidance

Enterprise-level guidance

Data Classification Adoption Challenge

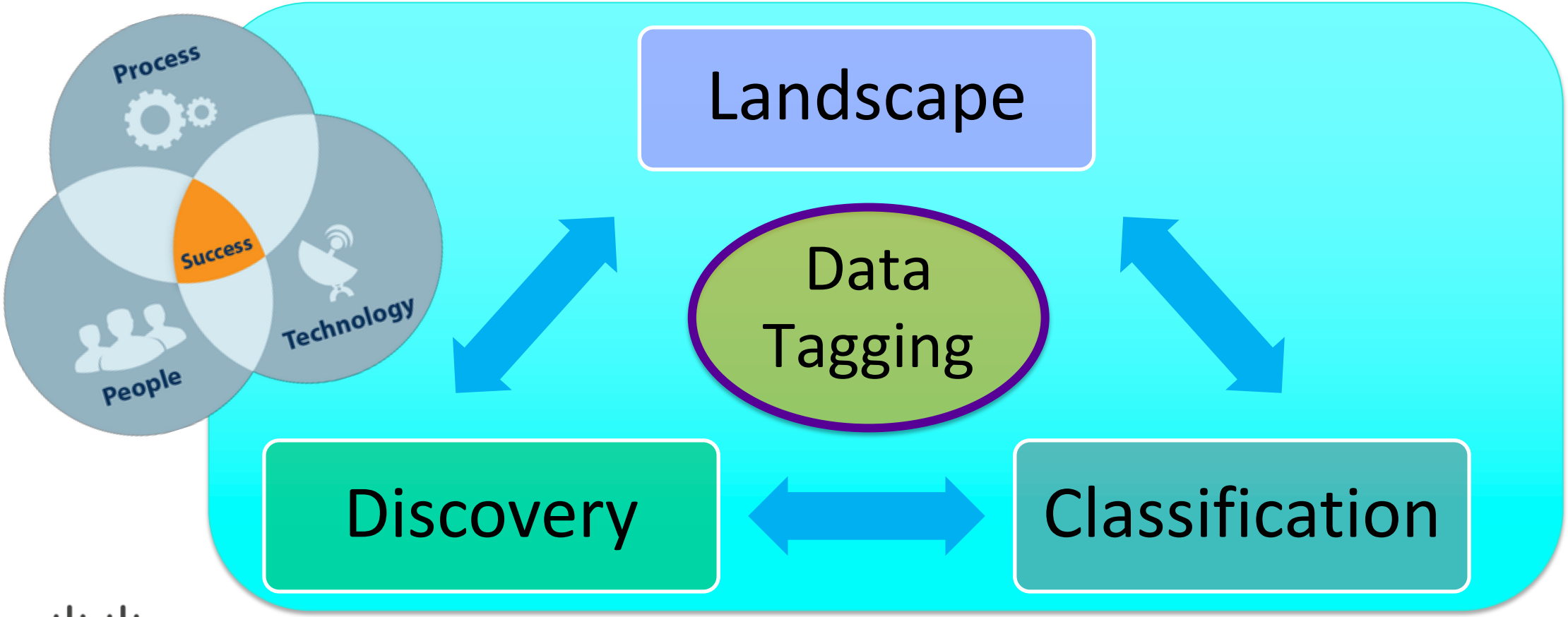


Enforcement: the Rubber hits the Road

Policy enforcement is predicated on accurate classification of the data

Data Identification Cohesion

Each area plays an important role in identifying data, but need to be aligned and to evolve cohesively

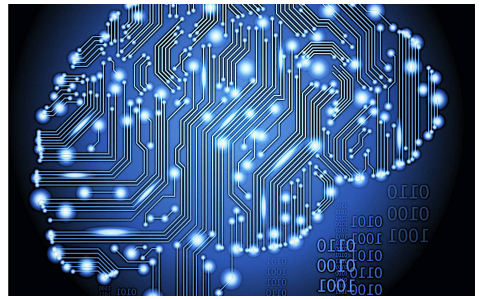


Building a bridge

Contextual classification provides the link to both user-generated and auto-classification tools and processes

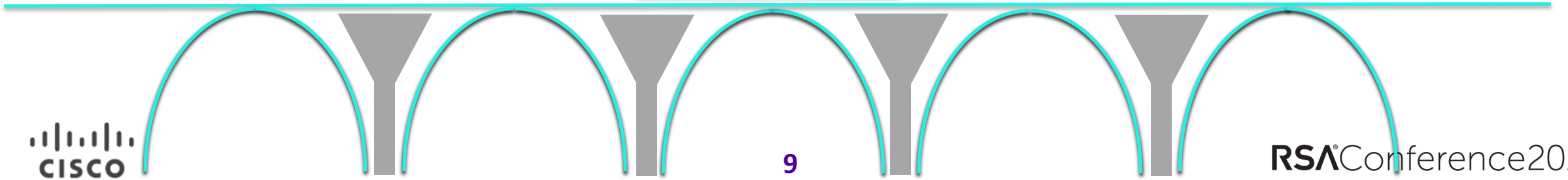
Data Users

Business Data Owners / Trustees



Machine Learning

User-generated classification ⟷ **Contextual Classification** ⟷ **Auto-Classification**



RSAConference2019

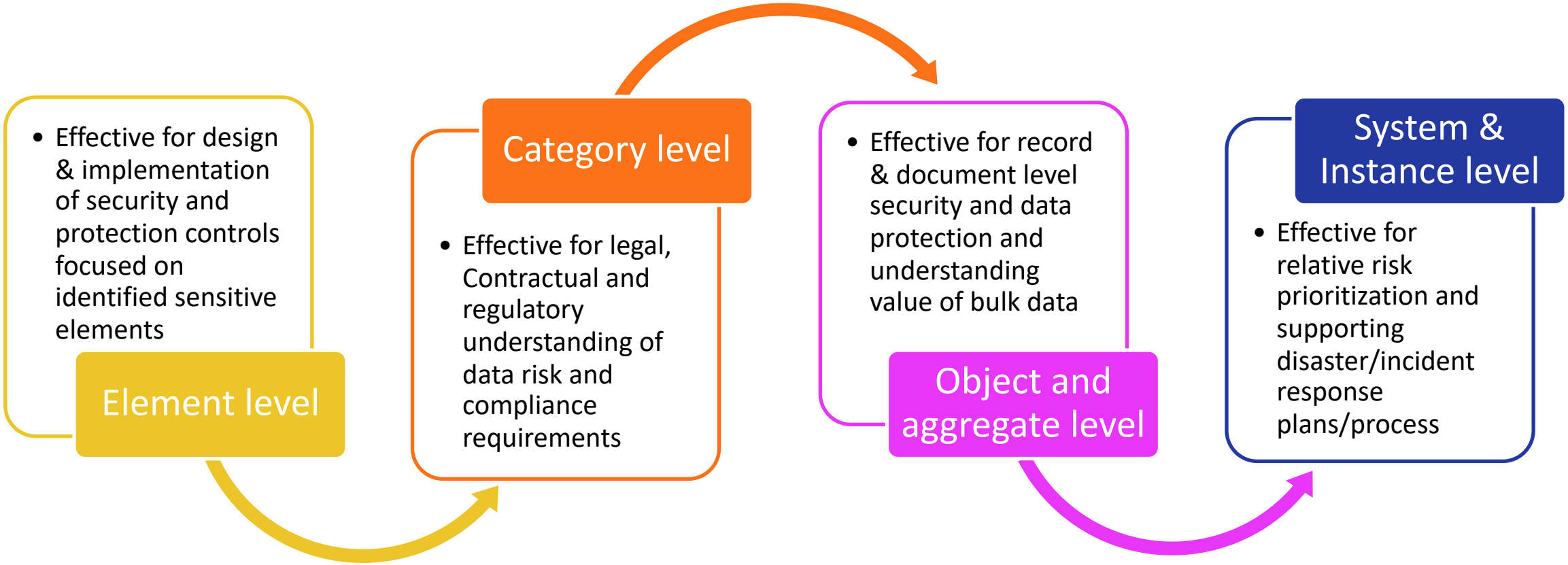
Contextual Data Classification

Use-case based approach

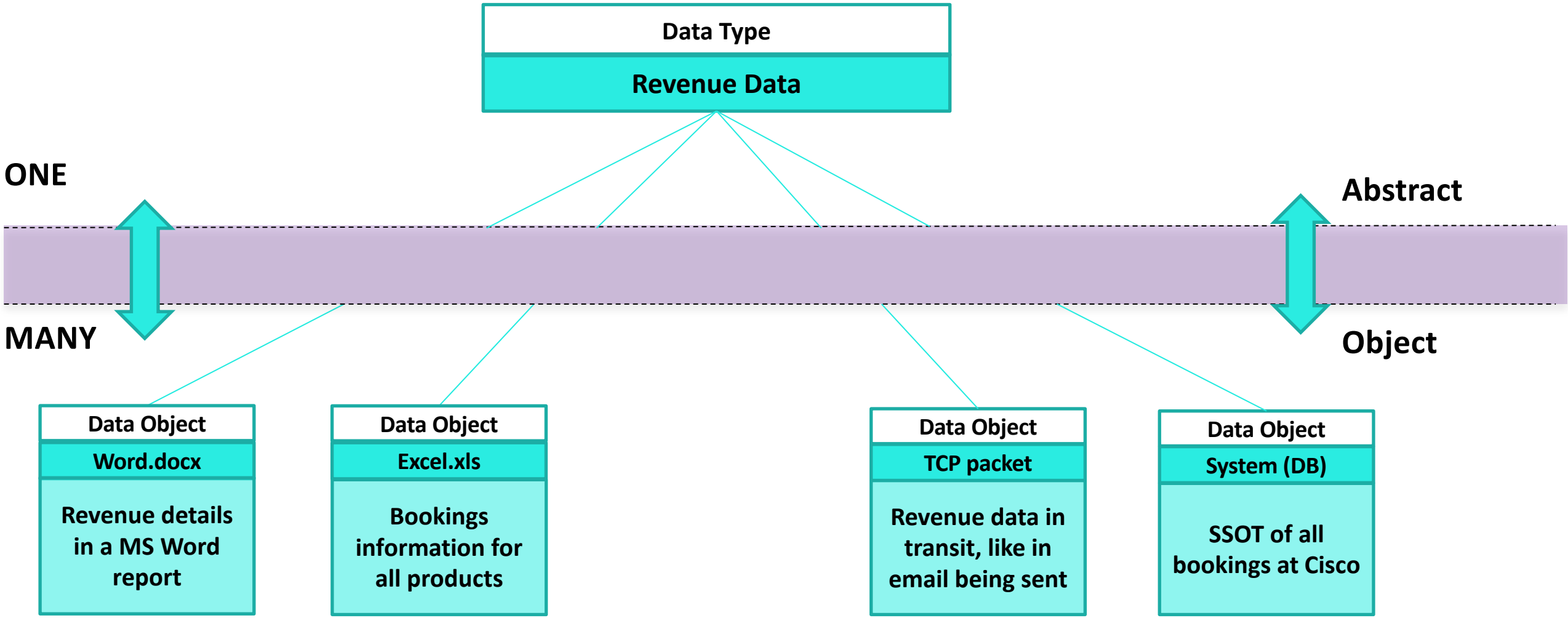
How To Apply The Model

- Building decision/context models
  - Step 1 (a, b, c): Identify the correct unit of processing and protection, & business relevance
  - Step 2: Extracting context
  - Step 3: Building the model
- Preserving context and acceptable use of data (getting ready to apply policies)
  - Step 4: Preserving classification with ability to scale/align with future vision, and planning enforcement of acceptable use
  - Step 5: Overall approach
- Use-case specific architecture for applying the right controls (to achieve enforceability)
  - Step 6: Accurate Guidance for data users to handle and share data

Step 1 (a): Identifying the correct unit of processing and data protection



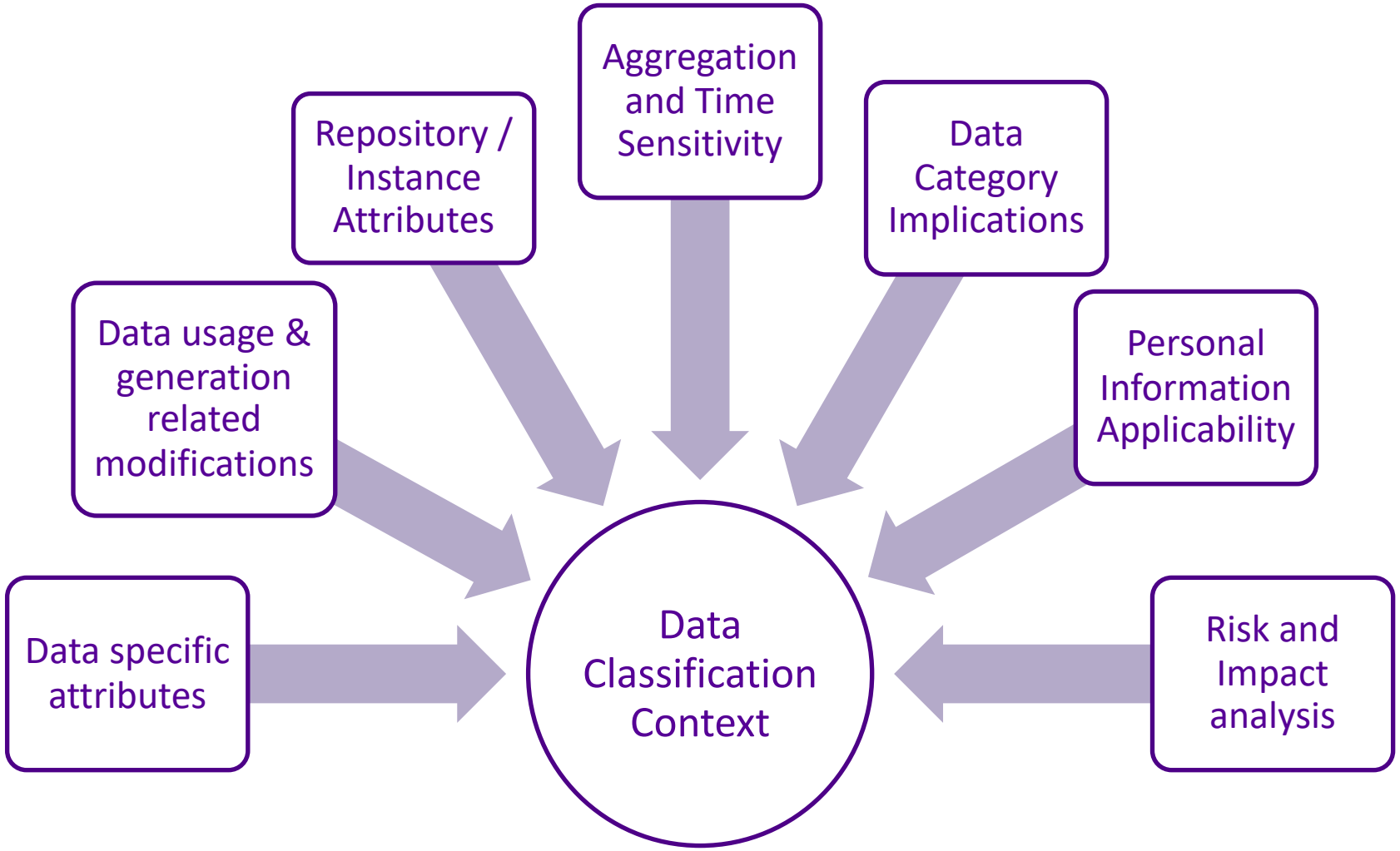
Step 1 (b): Identifying the correct data object for context extraction



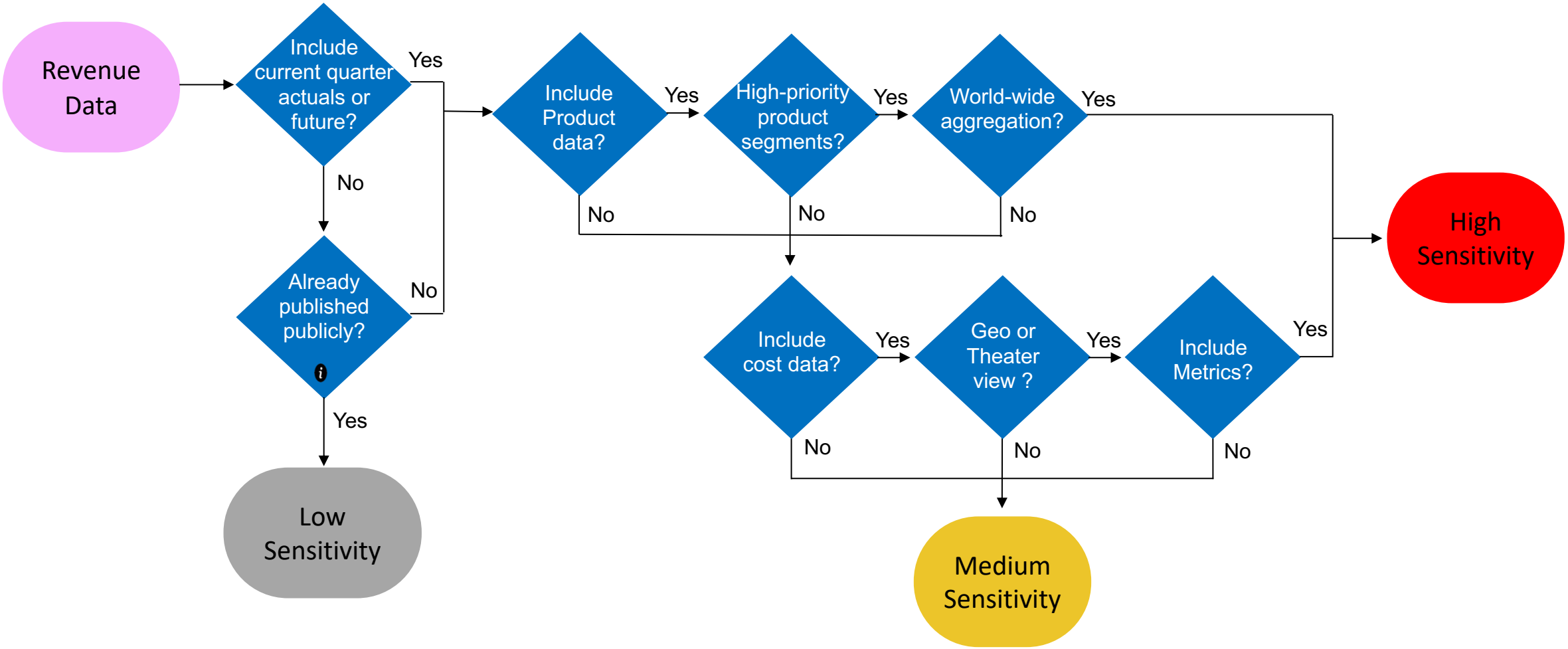
Step 1 (c): Business relevance of contextual classification

- Identify data objects which are good candidates for contextual classification based on business relevance (business defined attributes)
  - Mission criticality
  - Volume of data
  - Count of users
  - PII or Non PII
- Not all data objects will be good candidates for contextual classification
  - Static data classification
  - Not being the correct unit of data processing or protection

Step 2: Extracting context - Asking the right questions



Step 3: Building the model with the owners of the data



Step 4: Preserving context and applying the right controls

Need a comprehensive business solution in support of "Classify Before Use" paradigm…

- *Data must be classified before its use*
- *Data must be classified when it is created, if possible*
- *Classification level must evolve to reflect business context changes*

Three key activities define the Classification solution:

Determine
Assess classification level of data

- **In-line**
  within business process when data is created / collected
- **Offline**
  - Historical data
  - Bulk data collection
  - e.g. Auto-Class

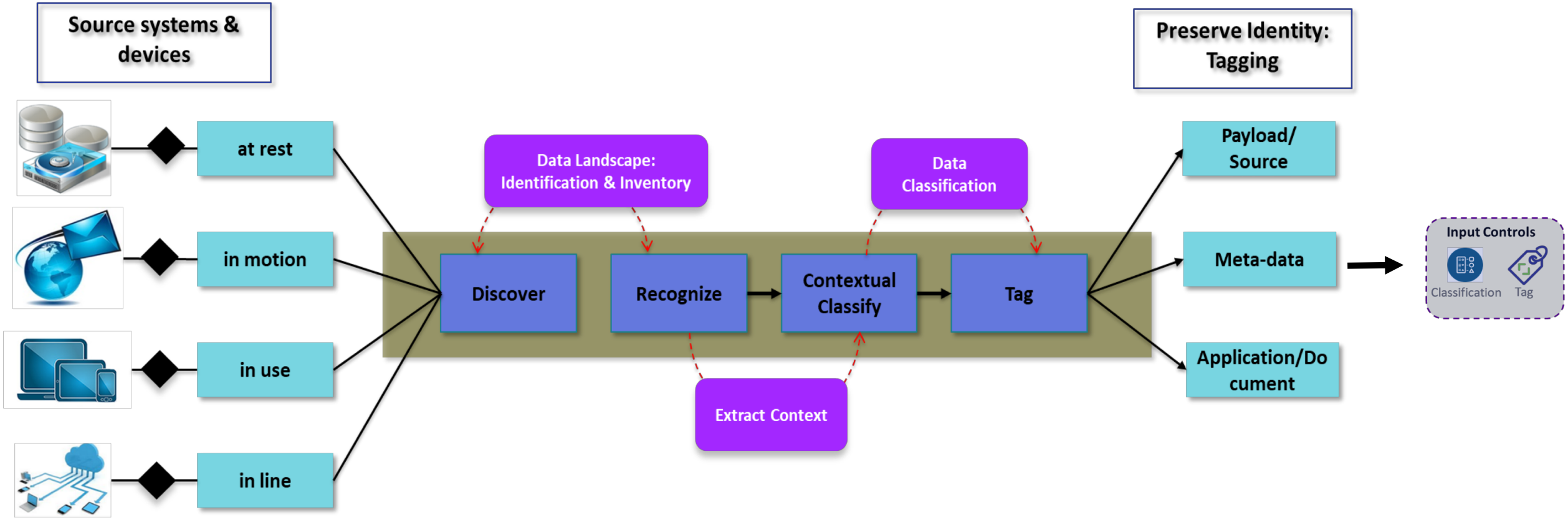
Reference
Access the classification level

- **Tagging**
  - Data structure extension
  - In-line metadata attribution (unstructured data)
- **Indexing, labelling**

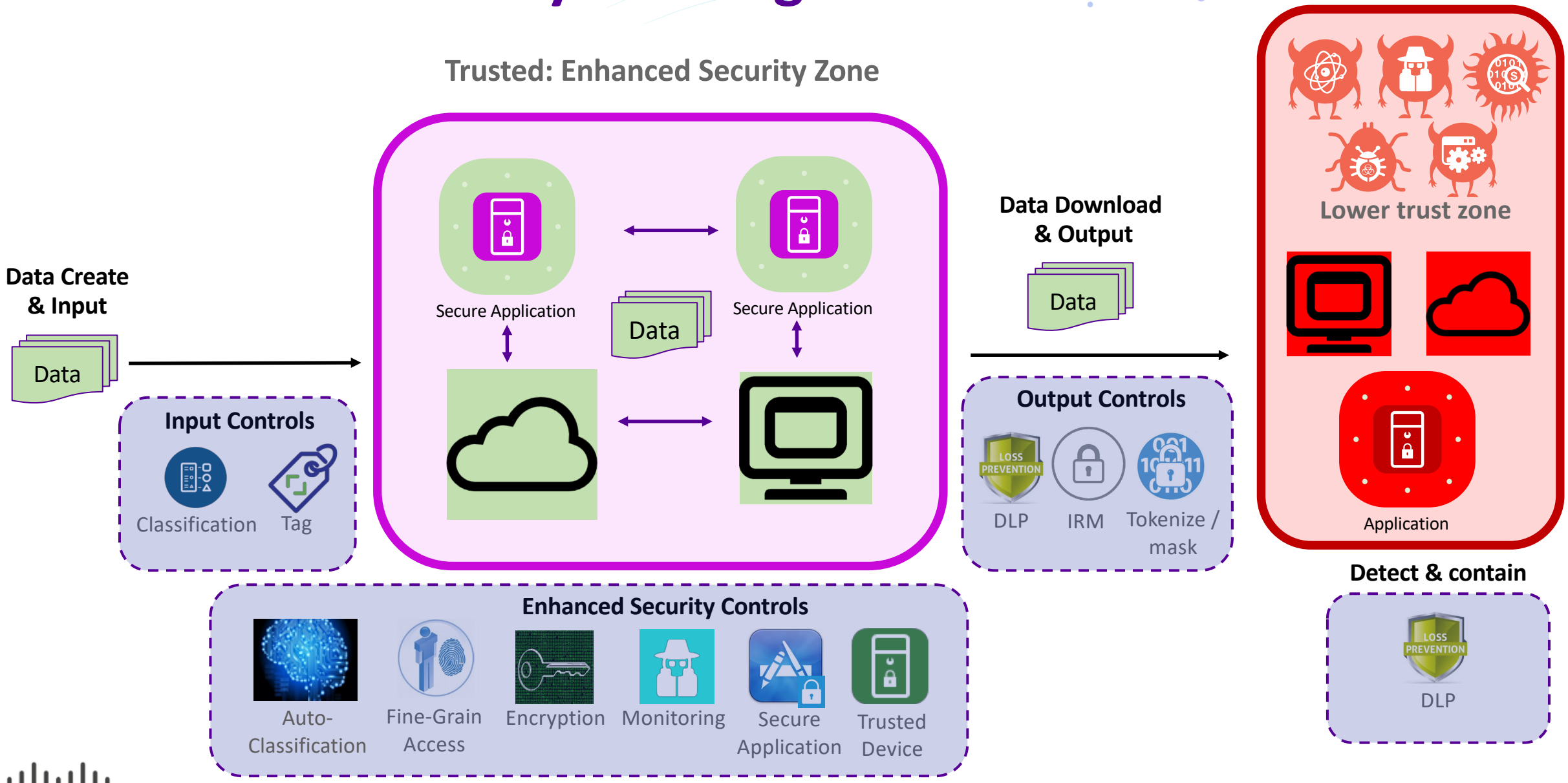
Enforce
Apply data protection controls

- **Data Loss Prevention (DLP)**
- **Data Monitoring**
- **Application logic**
- **Policy-controlled rules engine**

Step 5: Overall Approach

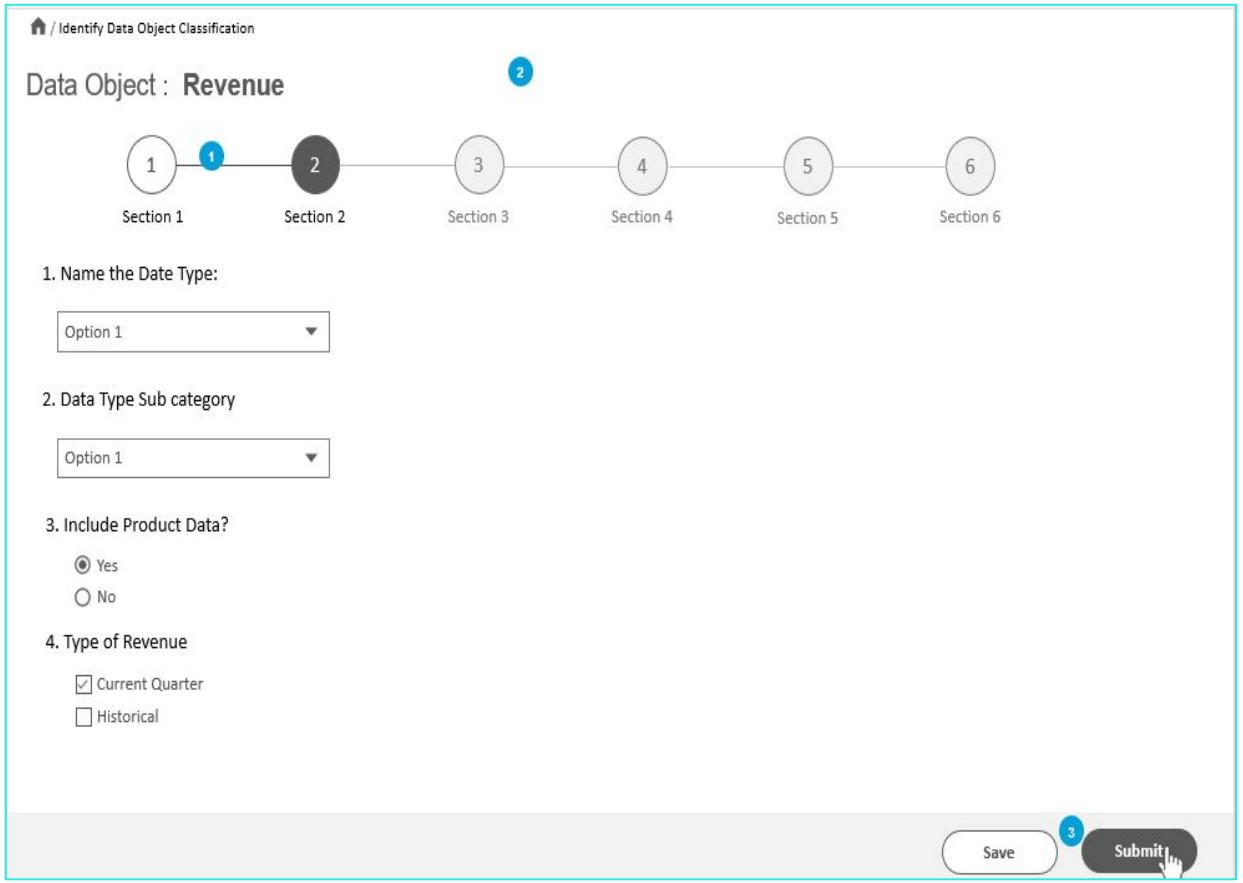


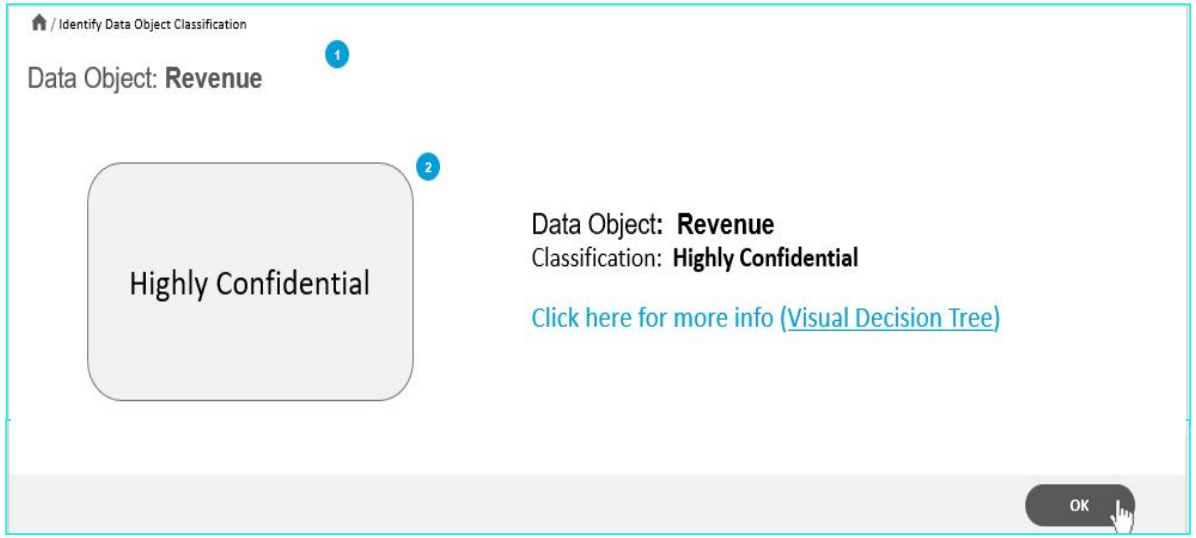
Enhanced data security building blocks



Slide Credit: Gerwin Tijink, Cisco Systems

Step 6: Accurate guidance for users using the model





RSAConference2019

Q&A

Anchit Arora
Program Manager
Cisco
@ancarora

John Cashman
Information Security Architect
Cisco
@jdcashman