

INFORMATION SECURITY CLASSIFICATION



Information Security Classification

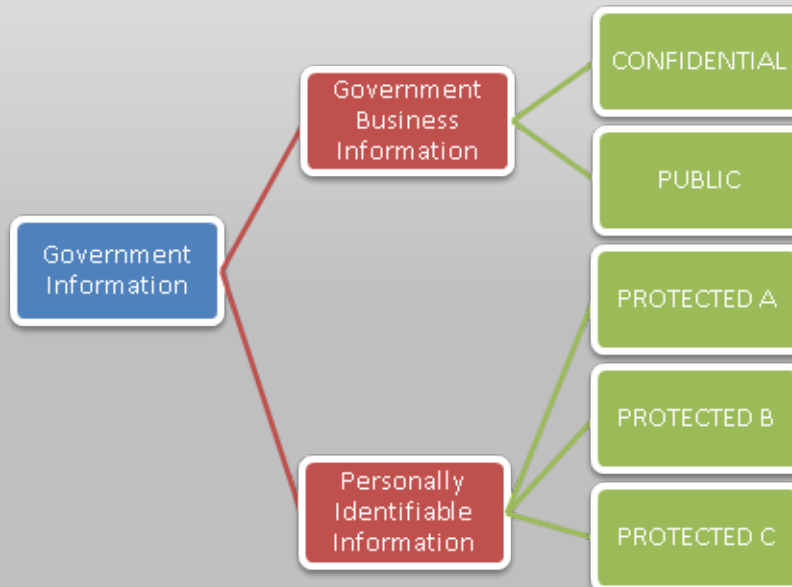
- Classification Schemes
- Drivers for Change
- Targets
- Players
- Classification Steps
- Models – Domain, Logical, Physical
- Next steps
- Questions

Data Classification Schemes

- **Current**

Level	Considerations (for all levels)	Labels
High	Financial Harm	Cabinet Confidential, High Sensitivity
Medium	Operational Harm	Medium Sensitivity, Personal*
Low	Personal Harm	Low Sensitivity, Public

- **New**



Drivers for change

- Confusion
- Practical Use
- Privacy Management and Accountability Program (PMAP) requirement
 - Personal Information Inventories
 - Clear understanding of what contactors have access to what personal information

Targets

- Databases*
- NRPP Document Management System*
- LAN
- Others?

Structured vs Unstructured

Players

- Data Custodians
 - Business Area reps
- Business Portfolio Managers (or PMs/BAs)
- Information Security
- Privacy (MPO, PCT)
- Database Administrators
- Data Architecture



Schema A

Table A

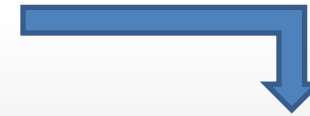
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5
Attribute 6

Table B

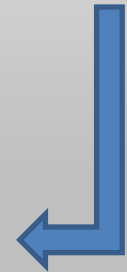
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5

Table C

Attribute 1 PK
Attribute 2 FK
Attribute 3
Attribute 4
Attribute 5
Attribute 6



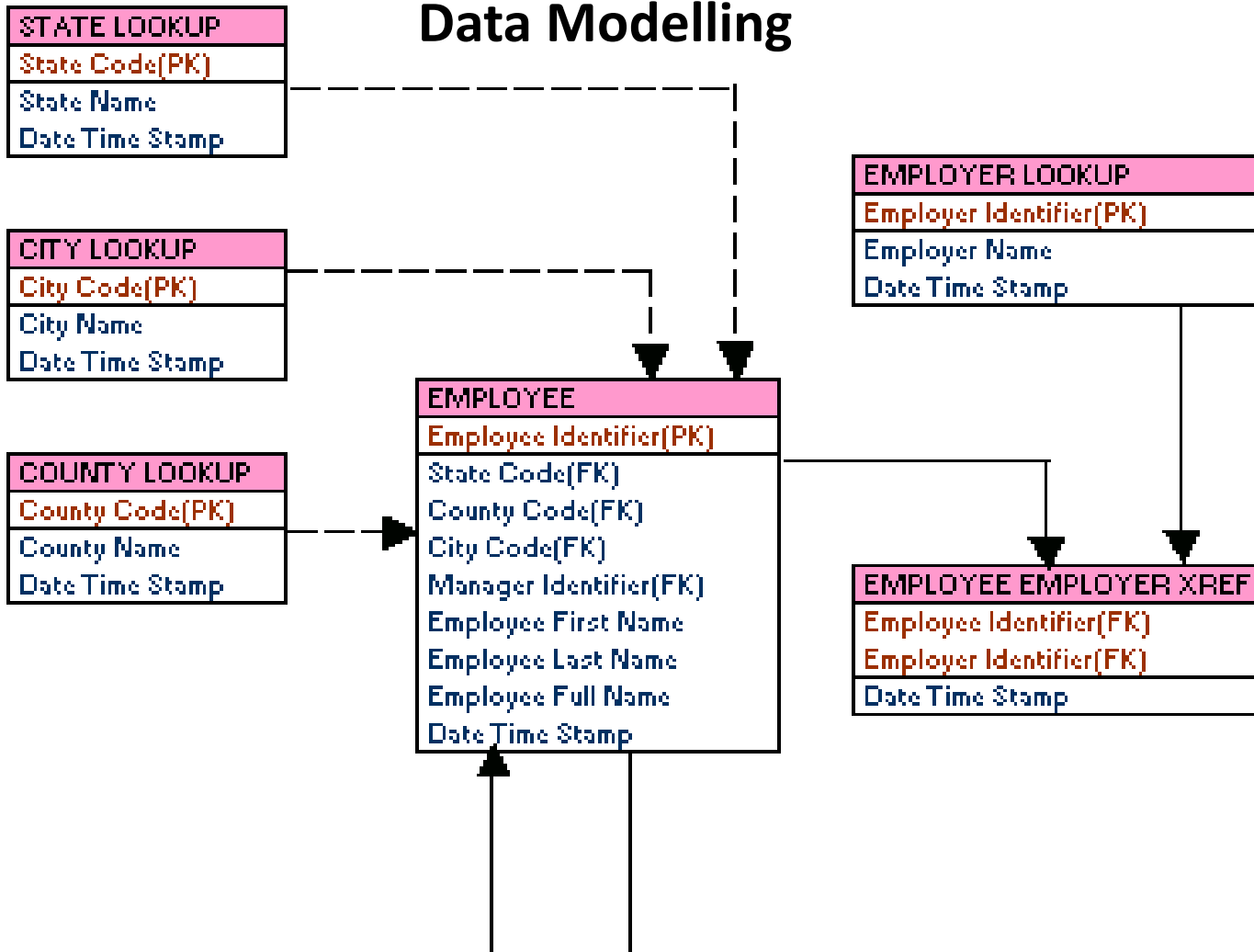
Schema	Table	Column	Data Type	Column Length	Nullable	Rows in Table	Information Security Classification
TRAX	TRFMRPTY	CLI_LONG_ADDR_ONE	VARCHAR2	45	N	951	PROTECTED_A
TRAX	TRFMRPTY	CLI_LONG_ADDR_TWO	VARCHAR2	45	N	35	PROTECTED_A
TRAX	TRFMRPTY	CLI_ALI_PERS_DRIVERS	VARCHAR2	25	N	6	PROTECTED_B
TRAX	TRFMRPTY	CLI_ALI_ADDR_2	VARCHAR2	25	N	153	PROTECTED_A
TRAX	TRFMRPTY	CLI_DEPT_NAME	VARCHAR2	25	N	885	PUBLIC
TRAX	TRFMRPTY	CLI_DRIVER_LICENSE	VARCHAR2	25	N	665	PROTECTED_B
TRAX	TRFMRPTY	CLI_EMPLOYER	VARCHAR2	25	N	885	PUBLIC
TRAX	TXRPMPTST	DAT_CLIENT_STAT_DESC	VARCHAR2	45	N	751	PUBLIC
TRAX	TXVLMTHOD	DAT_METHOD_OID	VARCHAR2	45	N	741	PUBLIC
TRAX	TXXPMBAL	CLI_ALT_EMAIL	VARCHAR2	50	N	77	PROTECTED_A
TRAX	TXXPMBAL	CLI_CATEGORY	VARCHAR2	1	N	2	CONFIDENTIAL
TRAX	TXXPMBAL	CLI_GETS_FINANCE_ORG	VARCHAR2	1	N	6505	CONFIDENTIAL
TRAX	TXXPMBAL	CLI_GETS_STMENT_ORG	VARCHAR2	1	N	12589	CONFIDENTIAL
TRAX	TXXPMBAL	OBS_SAVE_HISTORY	INT	1	N	99	CONFIDENTIAL
TRAX	TXVLCASE	CAS_STORAGE_ADDR_1	VARCHAR2	50	N	61321	PUBLIC
TRAX	TXVLCASE	CAS_STORAGE_ADDR_2	VARCHAR2	50	N	215	PUBLIC
TRAX	TXVLMTHOD	DAT_METHOD_BARCODE	INT	50	N	0	PUBLIC
VADD5	VETPMRPTY	CLI_EMPLOYER_CITY	VARCHAR2	25	N	885	PUBLIC



Example dataset

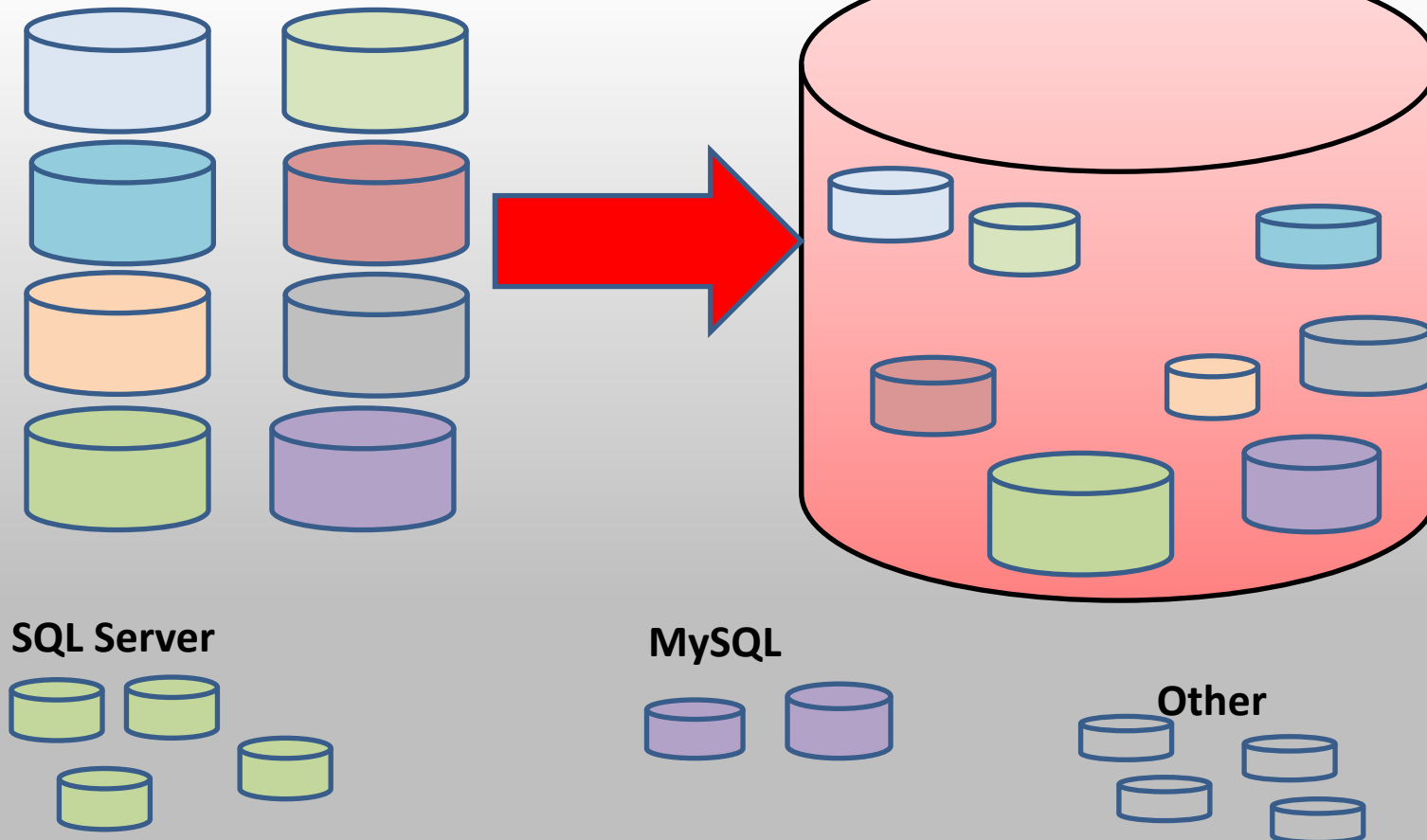
Schema	Table	Column	Data Type	Column Length	Nullable	Rows in Table	Information Security Classification
TRAX	TRPMRPTY	CLI_LONG_ADDR_ONE	VARCHAR2	45	N	951	PROTECTED_A
TRAX	TRPMRPTY	CLI_LONG_ADDR_TWO	VARCHAR2	45	N	35	PROTECTED_A
TRAX	TRPMRPTY	CLI_ALT_PERS_DRIVERS	VARCHAR2	25	N	6	PROTECTED_B
TRAX	TRPMRPTY	CLI_ALT_ADDR_2	VARCHAR2	25	N	153	PROTECTED_A
TRAX	TRPMRPTY	CLI_DEPT_NAME	VARCHAR2	25	N	885	PUBLIC
TRAX	TRPMRPTY	CLI_DRIVER_LICENSE	VARCHAR2	25	N	665	PROTECTED_B
TRAX	TRPMRPTY	CLI_EMPLOYER	VARCHAR2	25	N	885	PUBLIC
TRAX	TXRPMPATST	DAT_CLIENT_STAT_DESC	VARCHAR2	45	N	751	PUBLIC
TRAX	TXVLMTHOD	DAT_METHOD_OID	VARCHAR2	45	N	741	PUBLIC
TRAX	TXXPMRALT	CLI_ALT_EMAIL	VARCHAR2	50	N	77	PROTECTED_A
TRAX	TXXPMRBAL	CLI_CATEGORY	VARCHAR2	1	N	2	CONFIDENTIAL
TRAX	TXXPMRBAL	CLI_GETS_FINANCE_CRG	VARCHAR2	1	N	6505	CONFIDENTIAL
TRAX	TXXPMRBAL	CLI_GETS_STMENT_CRG	VARCHAR2	1	N	12589	CONFIDENTIAL
TRAX	TXXPMRBAL	OBS_SAVE_HISTORY	INT	1	N	99	CONFIDENTIAL
TRAX	TXXVLCASE	CAS_STORAGE_ADDR_1	VARCHAR2	50	N	61321	PUBLIC
TRAX	TXXVLCASE	CAS_STORAGE_ADDR_2	VARCHAR2	50	N	215	PUBLIC
TRAX	TXXVLMTHOD	DAT_METHOD_BARCODE	INT	50	N	0	PUBLIC
TRAX	TXXPMRPTY	CLI_EMPLOYER_CITY	VARCHAR2	25	N	885	PUBLIC

Data Modelling

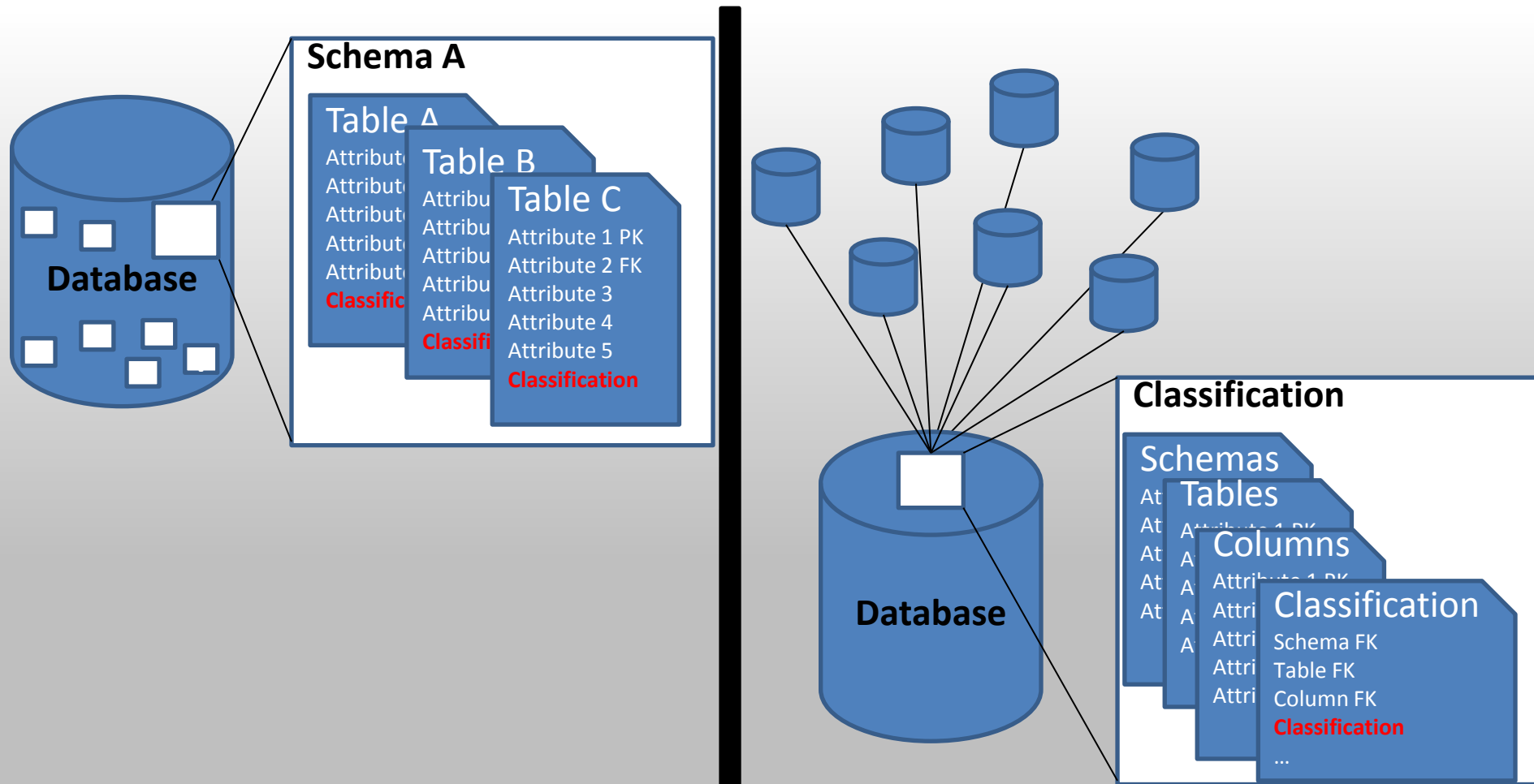


Oracle Databases

Exadata



How should we store classification details?

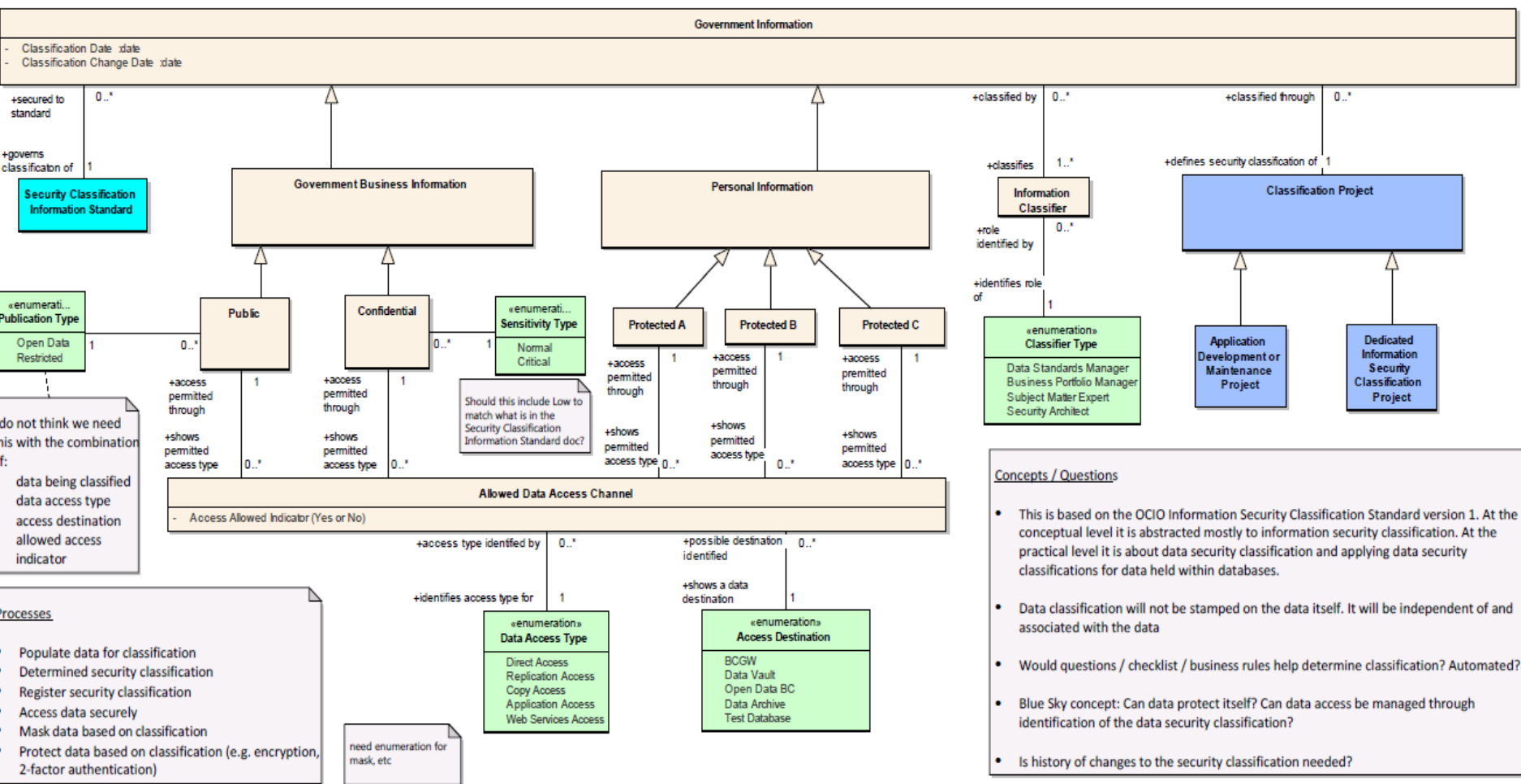


Domain Model

Information Security Classification - Conceptual

Legend

- Classification Information
- Values List
- External Reference
- Out of Scope



I do not think we need this with the combination of:

- data being classified
- data access type
- access destination
- allowed access indicator

Processes

- Populate data for classification
- Determined security classification
- Register security classification
- Access data securely
- Mask data based on classification
- Protect data based on classification (e.g. encryption, 2-factor authentication)

need enumeration for mask, etc

Should this include Low to match what is in the Security Classification Information Standard doc?

Concepts / Questions

- This is based on the OCIO Information Security Classification Standard version 1. At the conceptual level it is abstracted mostly to information security classification. At the practical level it is about data security classification and applying data security classifications for data held within databases.
- Data classification will not be stamped on the data itself. It will be independent of and associated with the data
- Would questions / checklist / business rules help determine classification? Automated?
- Blue Sky concept: Can data protect itself? Can data access be managed through identification of the data security classification?
- Is history of changes to the security classification needed?

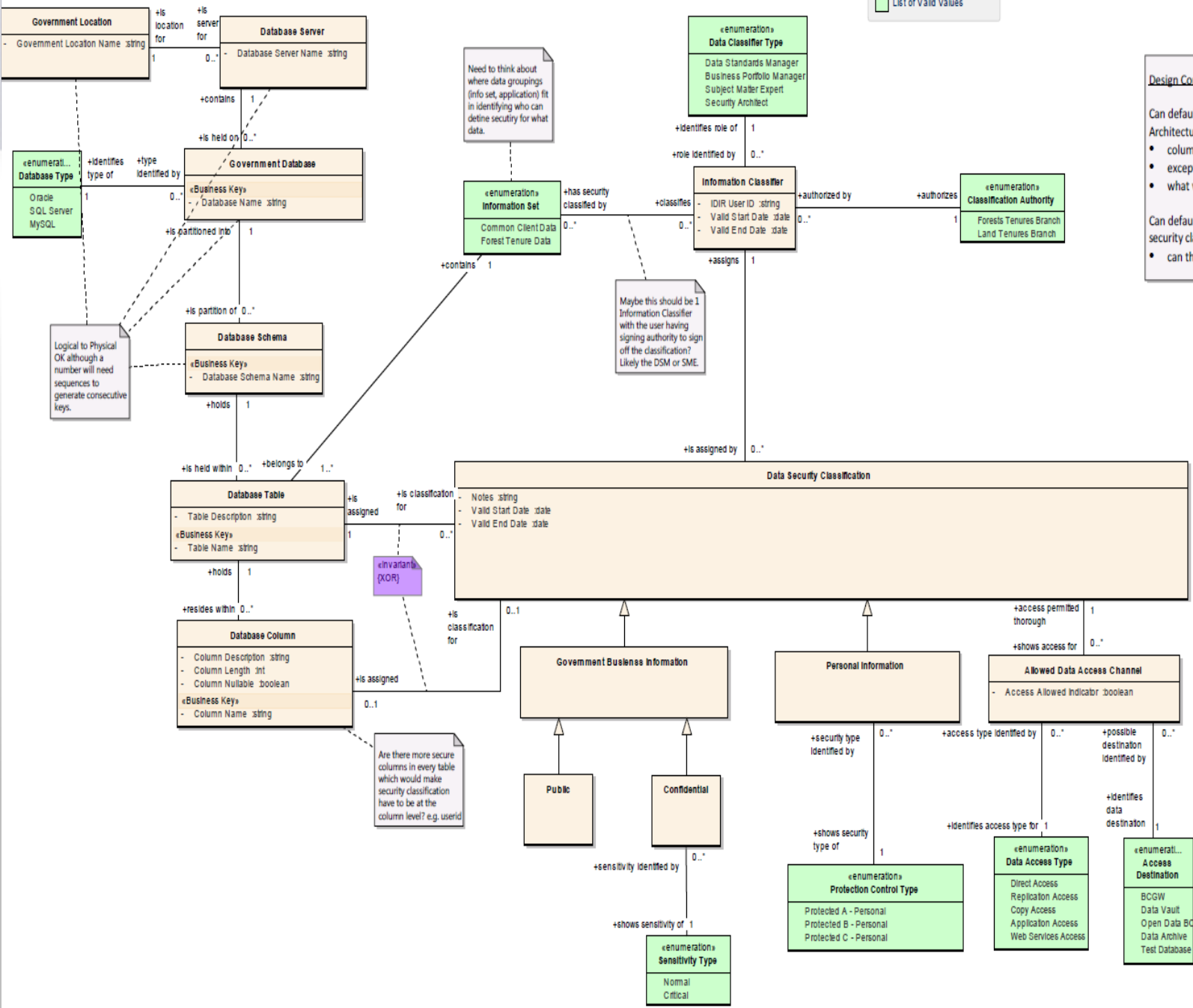
Data Architecture Advisory Council Questions

1. Does this need to cover row level security? See what direction is from Information Security Standard and Security Architects?
2. Does it need to cover a relaxed classification if the data ages out? - e.g. after 100 years data which was personal may be public
3. Could this also be used for to hold record retention information - ARCS/ORCS schedules, likely out of scope for initial project.

Logical Data Model

Legend

- Security Classification Class
- List of Valid Values



Need to think about where data groupings (info set, application) fit in identifying who can define security for what data.

Maybe this should be 1 Information Classifier with the user having signing authority to sign off the classification? Likely the DSM or SME.

Logical to Physical OK although a number will need sequences to generate consecutive keys.

Are there more secure columns in every table which would make security classification have to be at the column level? e.g. userid

Design Considerations - Exceptions Approach

Can default be table level security (to be determined by Security Architecture)

- column level security added as an exception
- exceptions defined specifically but not all columns
- what would benefits and drawbacks be for this approach?

Can default data access channels be defined for each data security class

- can these be defined and automatically generated?

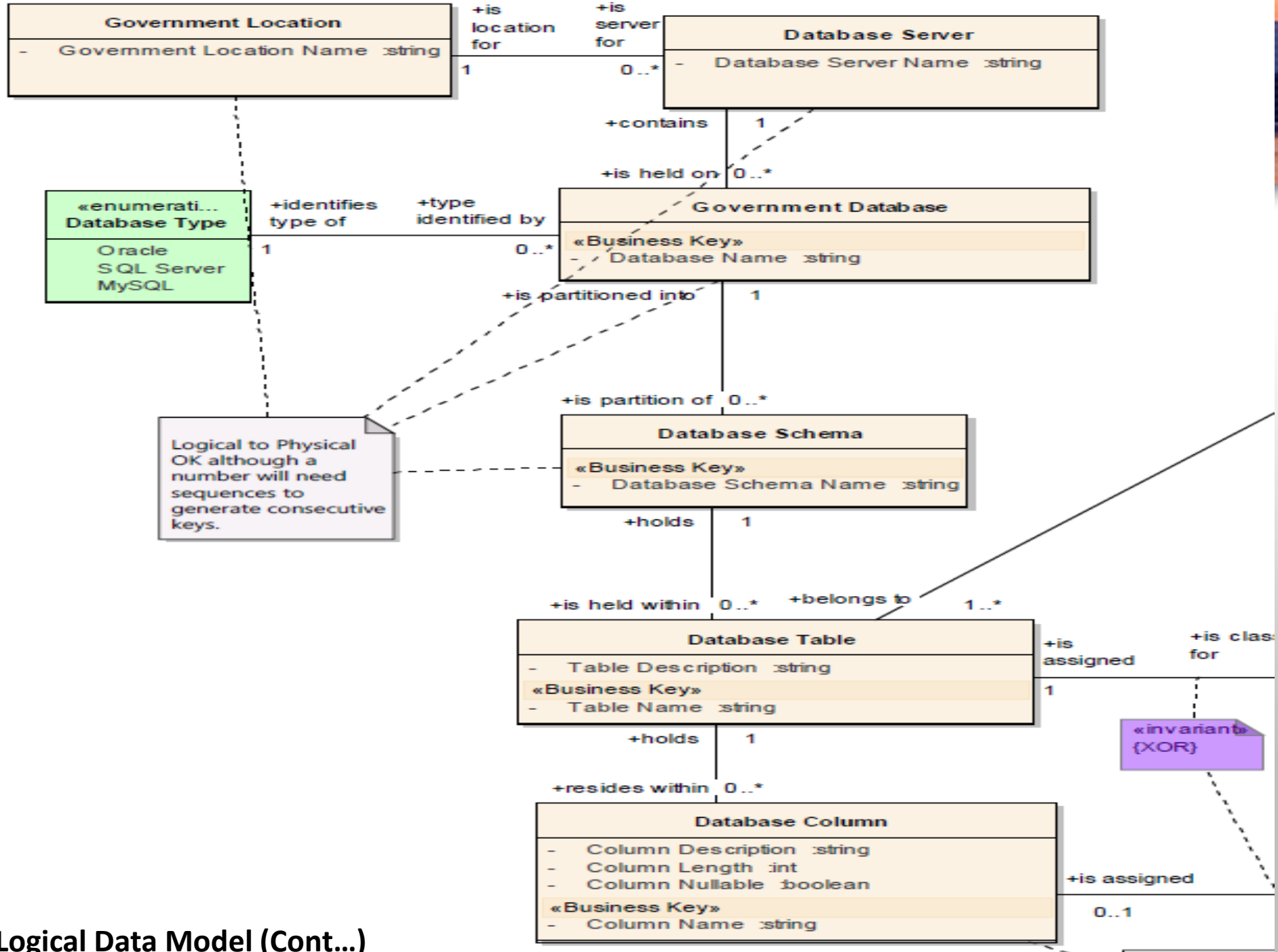
Design Considerations - Security Type

The sub-types might be designed as codes for the physical model:

- Information Type (code) - an enumeration which will be defined as Government Business Information or Personal Information
- Information Sensitivity (code) - either non-sensitive (Public) or sensitive (Confidential)
- Public Information Availability (code) - Open or Restricted
- Confidential Information Sensitivity (code) - Normal or Critical
- these values need descriptions

OR

- Maybe just a Security Type Code of Public, Confidential or Personal and an optional Confidential Information Sensitivity (code) - Normal or Critical and optional Protection Control Type Code



Logical Data Model (Cont...)

Logical Data Model (Cont...)

Legend

- Security Classification Class
- List of Valid Values

Need to think about where data groupings (info set, application) fit in identifying who can define security for what data.

«enumeration»
Information Set

- Common Client Data
- Forest Tenure Data

«enumeration»
Data Classifier Type

- Data Standards Manager
- Business Portfolio Manager
- Subject Matter Expert
- Security Architect

+identifies role of 1
+role identified by 0..*

Information Classifier

- IDIR User ID :string
- Valid Start Date :date
- Valid End Date :date

«enumeration»
Classification Authority

- Forests Tenures Branch
- Land Tenures Branch

+has security classified by 0..*

+classifies 0..*

+authorized by 0..*

+authorizes 1

contains 1

+assigns 1

Maybe this should be 1 Information Classifier with the user having signing authority to sign off the classification? Likely the DSM or SME.

+is assigned by 0..*

Data Security Classification

- Notes :string
- Valid Start Date :date
- Valid End Date :date

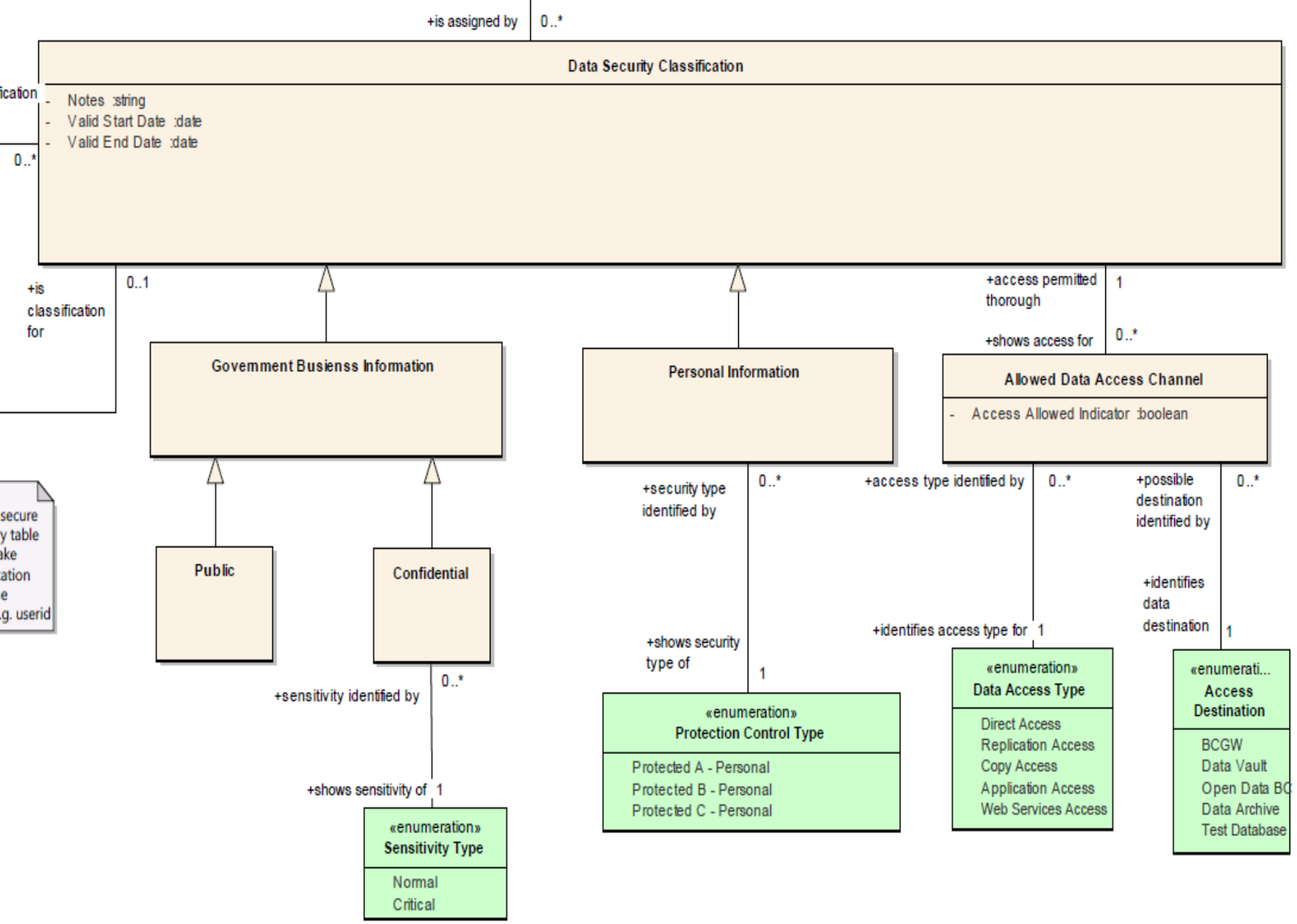
Design Considerations

- Can default Architecture
- column
- except
- what v
- Can default security cla
- can the

+is 0..1

+access permitted 1

Logical Data Model (Cont...)



Next Steps

- Working on physical implementation
- Integration into Data Modelling Standard
- Requirements on a user interface to facilitate classification using this structure
 - Short term (without UI, or very simple)
 - Longer term (client facing UI)

Questions?

