INFORMATION SECURITY CLASSIFICATION

Information Security Classification

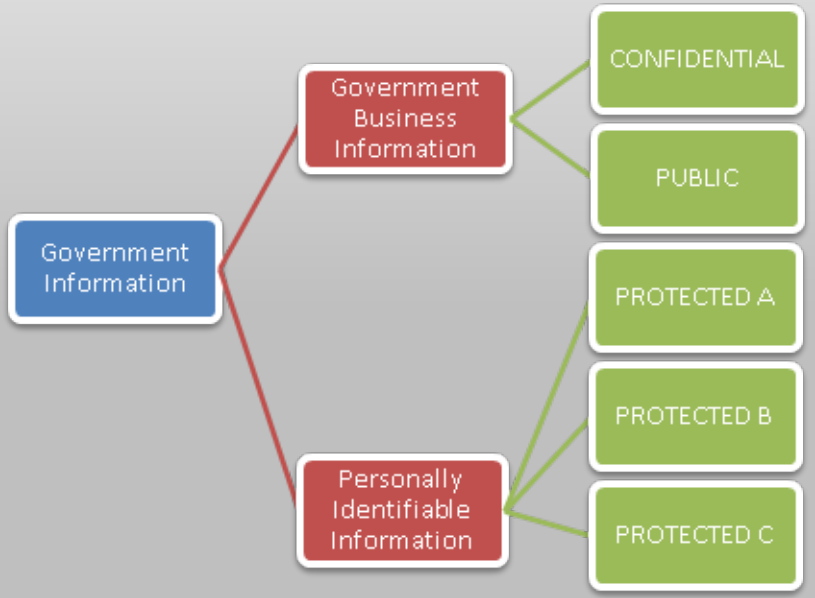
- Classification Schemes
- Drivers for Change
- Targets
- Players
- Classification Steps
- Models – Domain, Logical, Physical
- Next steps
- Questions

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**



Microsoft Word Document

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

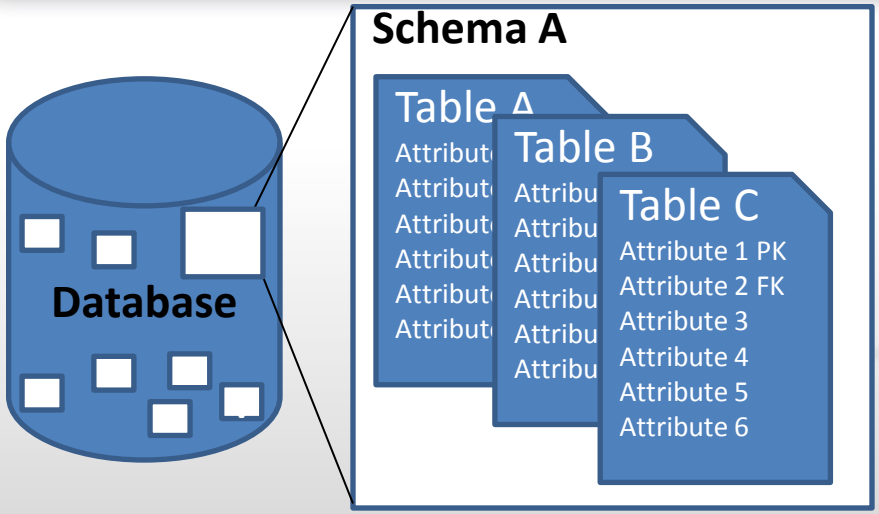
Targets

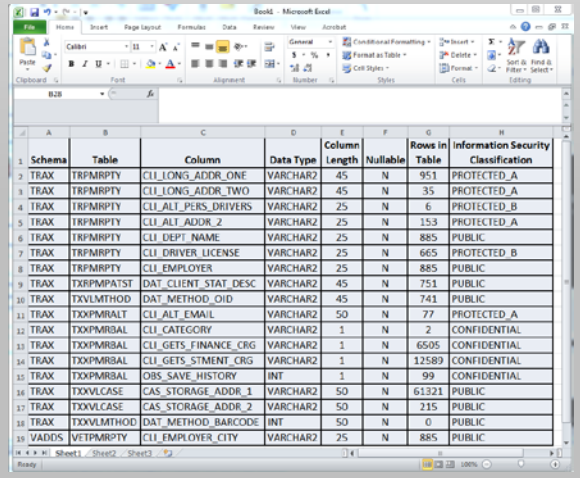
- Databases*
- NRPP Document Management System*
- LAN
- Others?

Structured vs Unstructured

Players

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



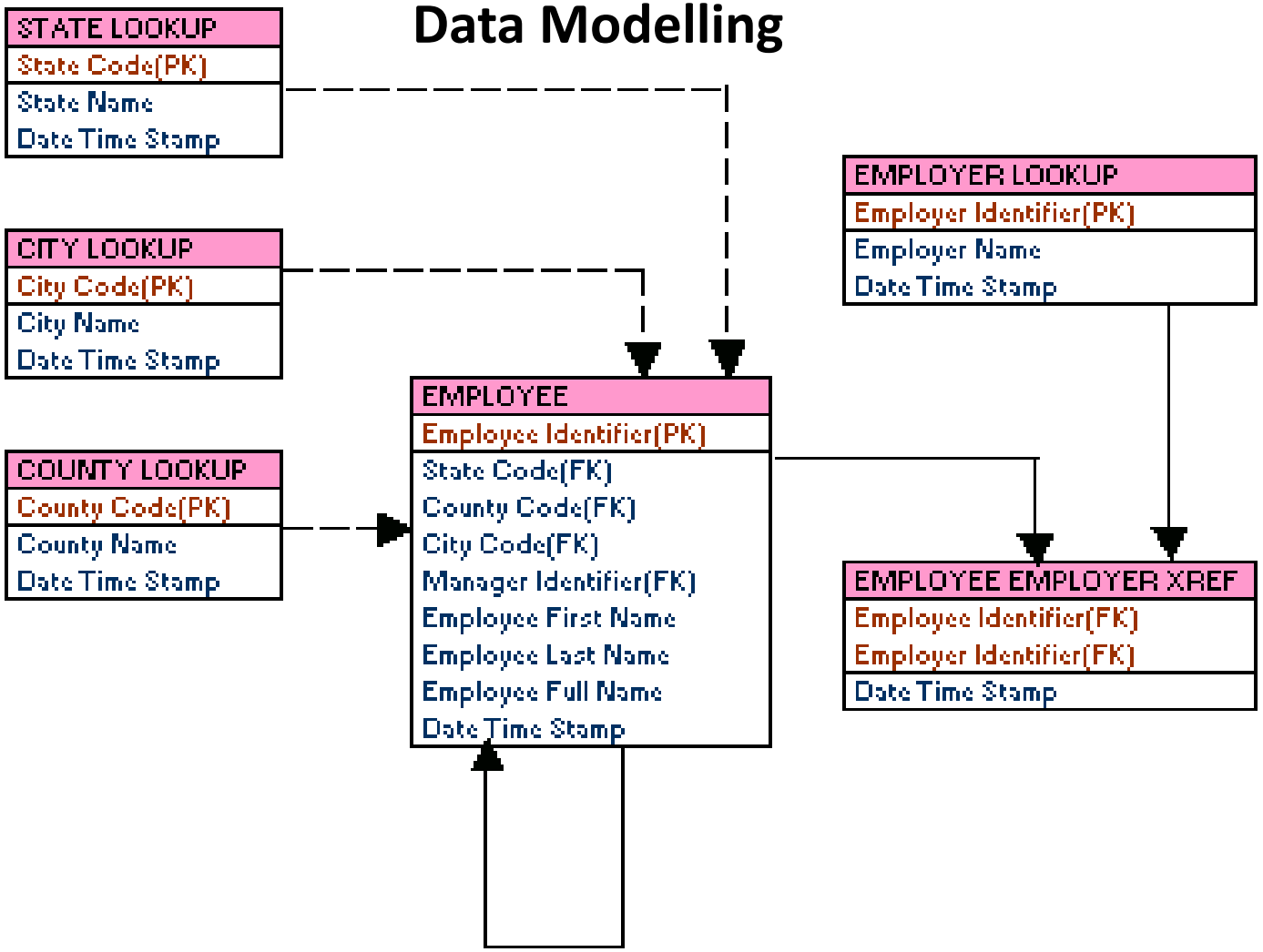


Schema	Table	Column	Data Type	Column Length	Nullable	Rows in Table	Information Security Classification
TRAX	TRPMRPTY	CLI_LONG_ADDR_ONE	VARCHAR2	45	N	951	PROTECTED_A
TRAX	TRPMRPTY	CLI_LONG_ADDR_TWO	VARCHAR2	45	N	35	PROTECTED_A
TRAX	TRPMRPTY	CLI_ALT_PERS_DRIVERS	VARCHAR2	25	N	6	PROTECTED_B
TRAX	TRPMRPTY	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
VADDS	VETPMRPTY	CLI_EMPLOYER_CITY	VARCHAR2	25	N	885	PUBLIC

Example dataset

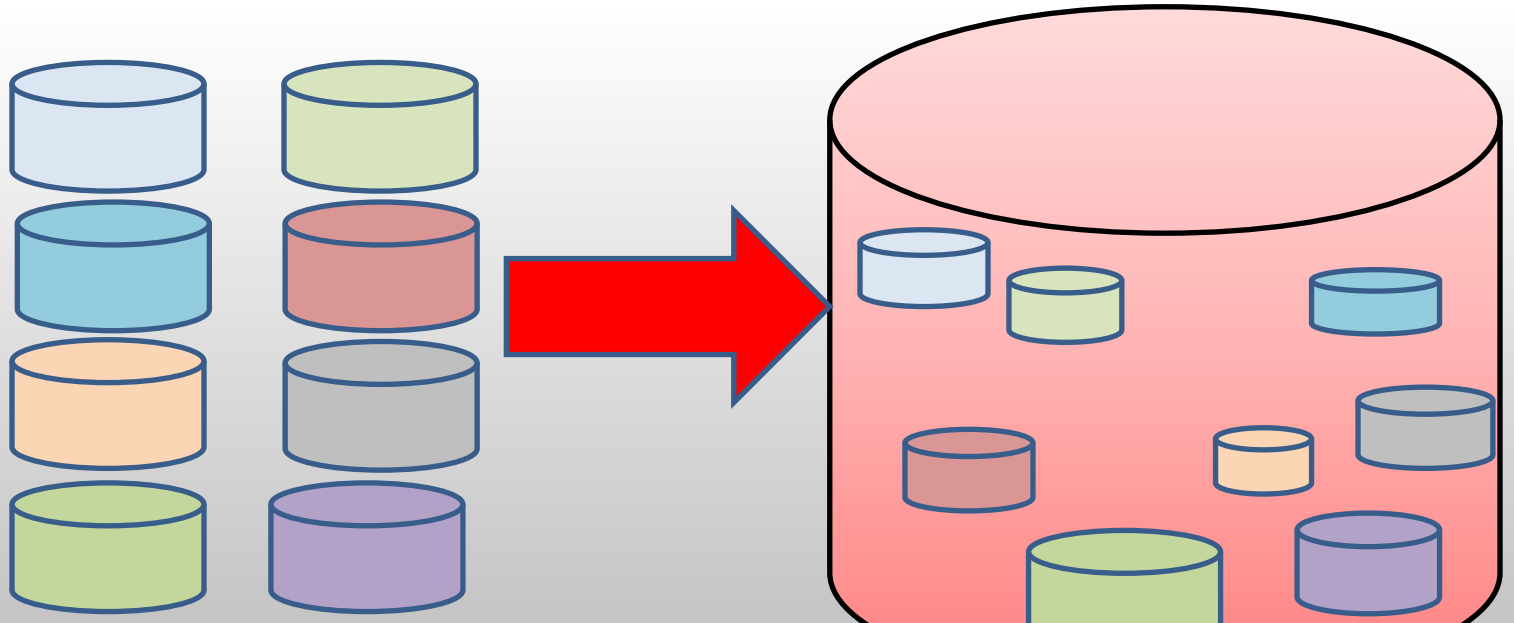
Schema	Table	Column	Data Type	Column Length	Nullable	Rows in Table	Information Security Classification
TRAX	TRPMRPTY	CLI_LONG_ADDR_ONE	VARCHAR2	45	N	951	PROTECTED_A
TRAX	TRPMRPTY	CLI_LONG_ADDR_TWO	VARCHAR2	45	N	35	PROTECTED_A
TRAX	TRPMRPTY	CLI_ALT_PERS_DRIVERS	VARCHAR2	25	N	6	PROTECTED_B
TRAX	TRPMRPTY	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

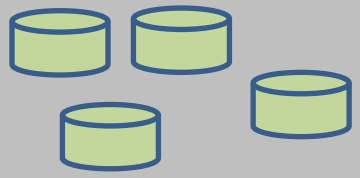


Oracle Databases

Exadata



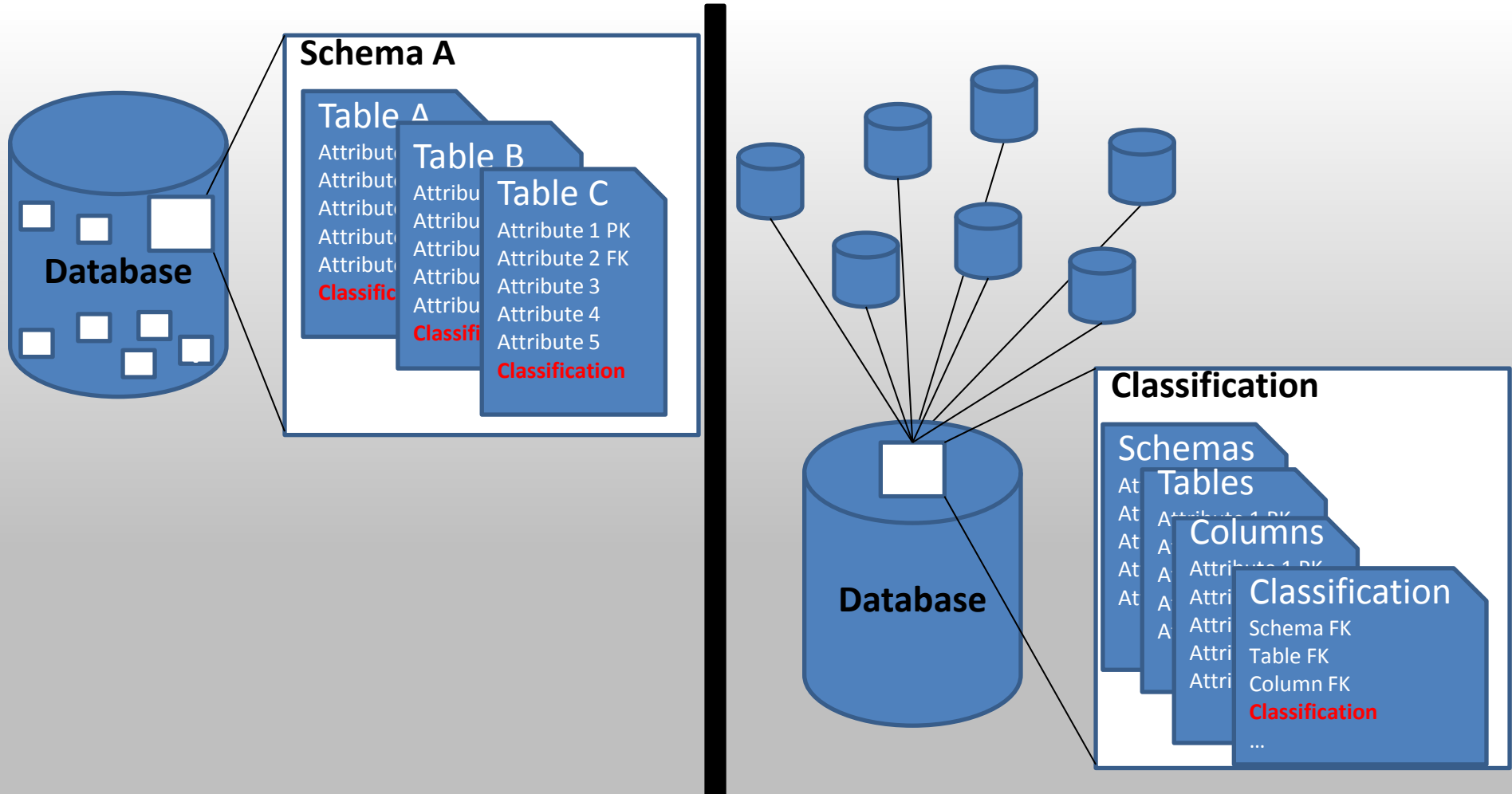
SQL Server



MySQL

Other

How should we store classification details?

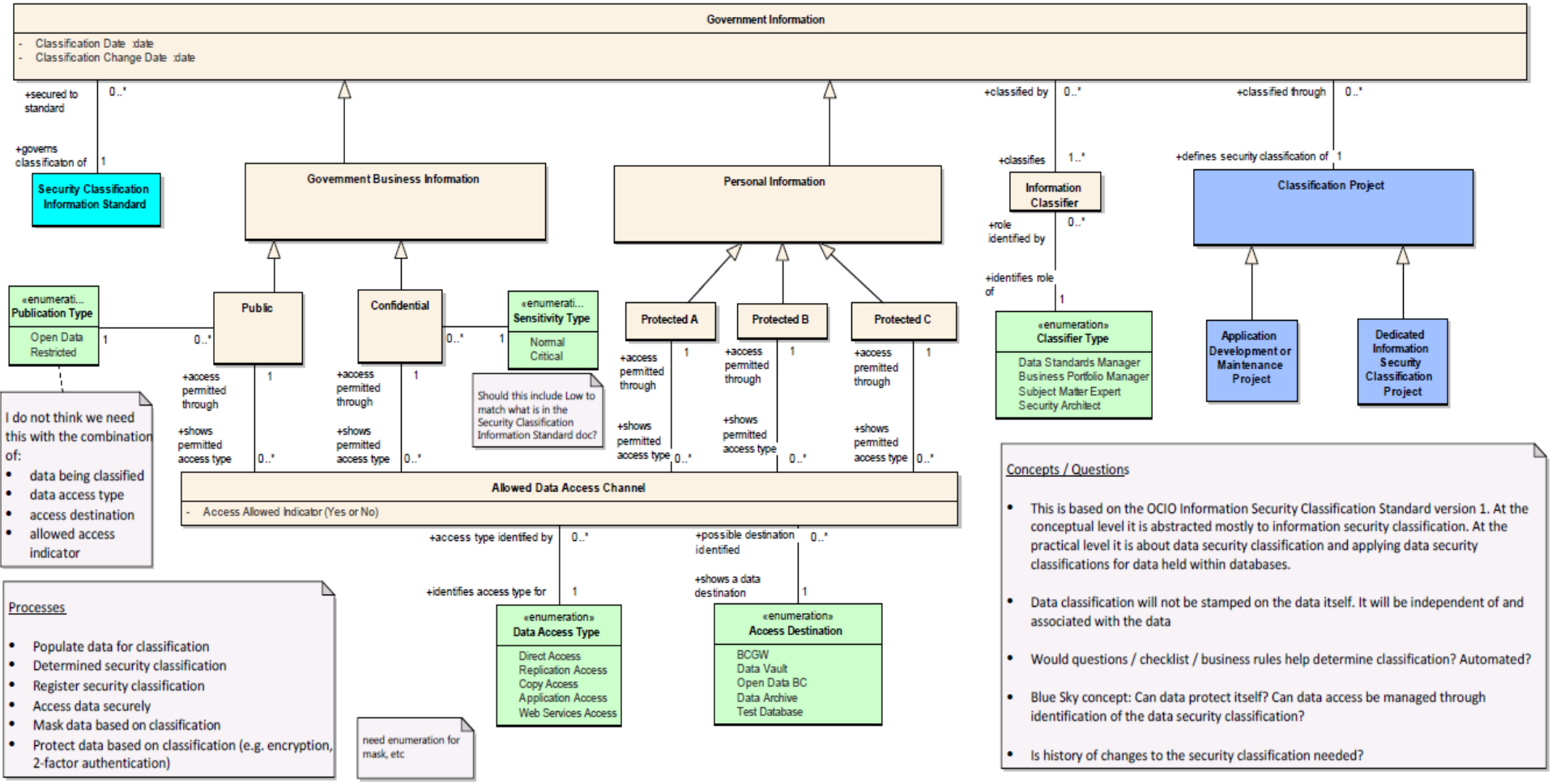


Name: Domain Objects - Information Classification Sketch 2
Package: Domain Objects
Version: 1.0
Author: tfulton

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)

Concepts / Questions

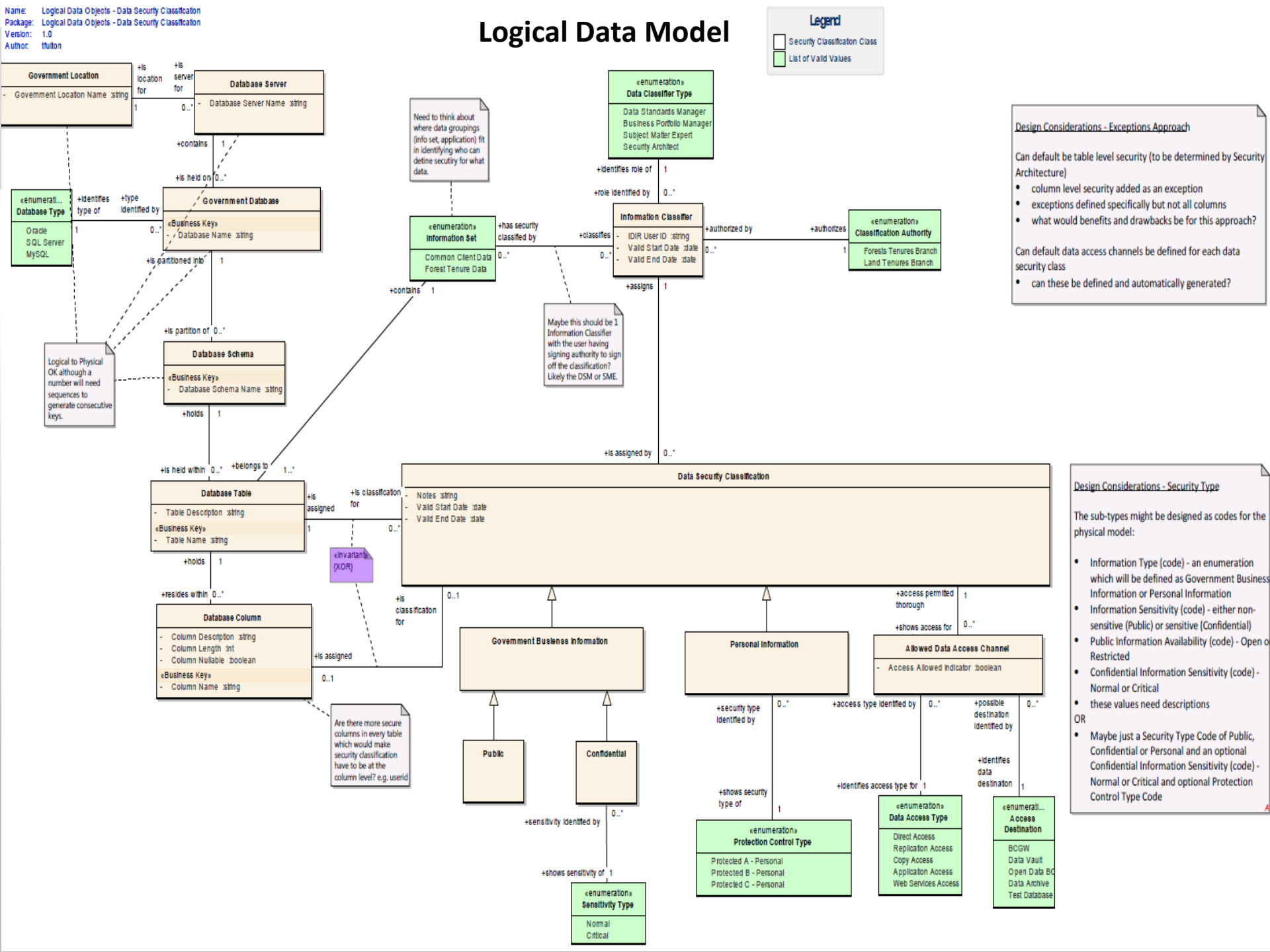
- This is based on the OCIO Information Security Classification Standard version 1. At the conceptual level it is abstracted mostly to information security classification. At the practical level it is about data security classification and applying data security classifications for data held within databases.
- 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?

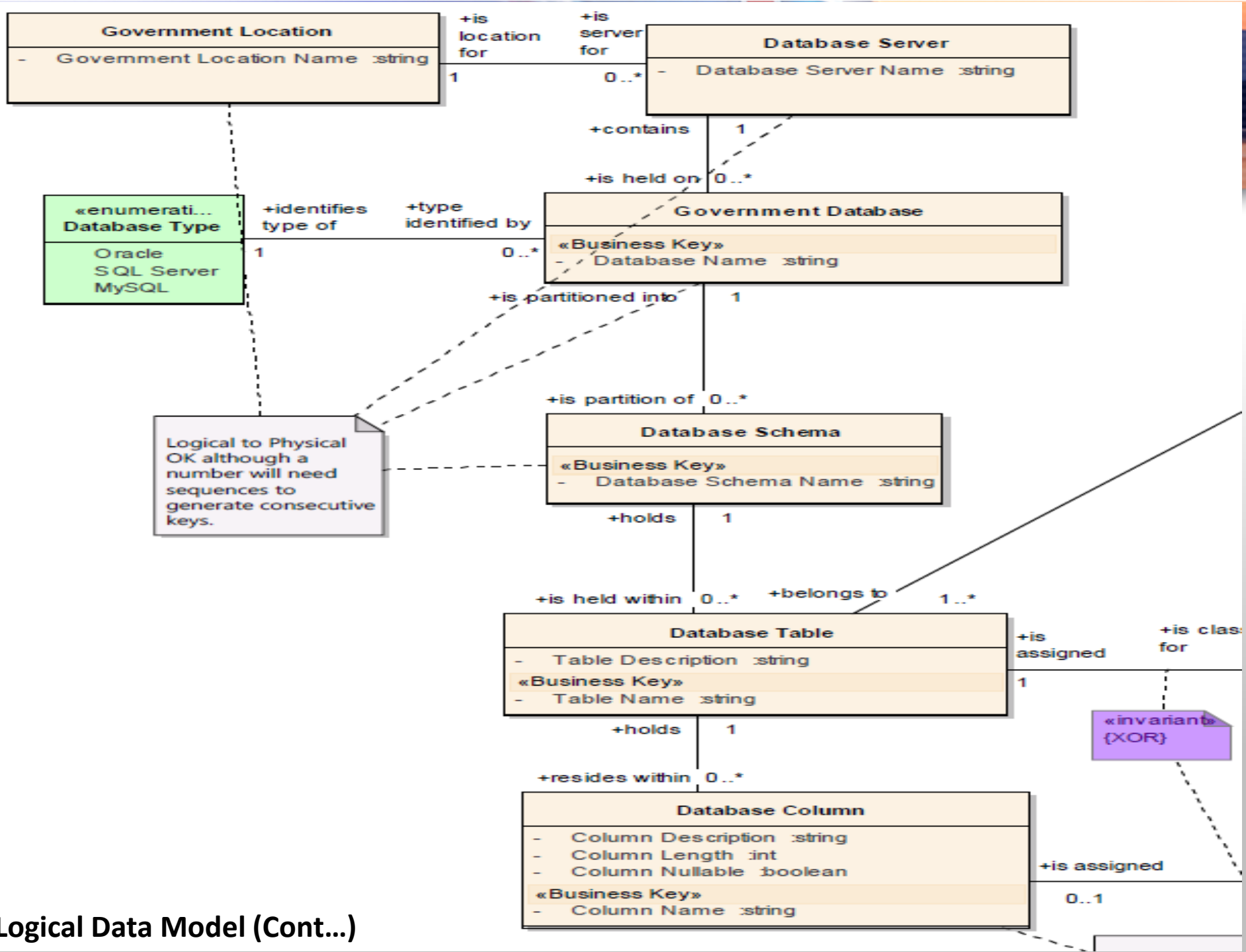
Data Architecture Advisory Council Questions

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.

Name: Logical Data Objects - Data Security Classification
Package: Logical Data Objects - Data Security Classification
Version: 1.0
Author: tfulton

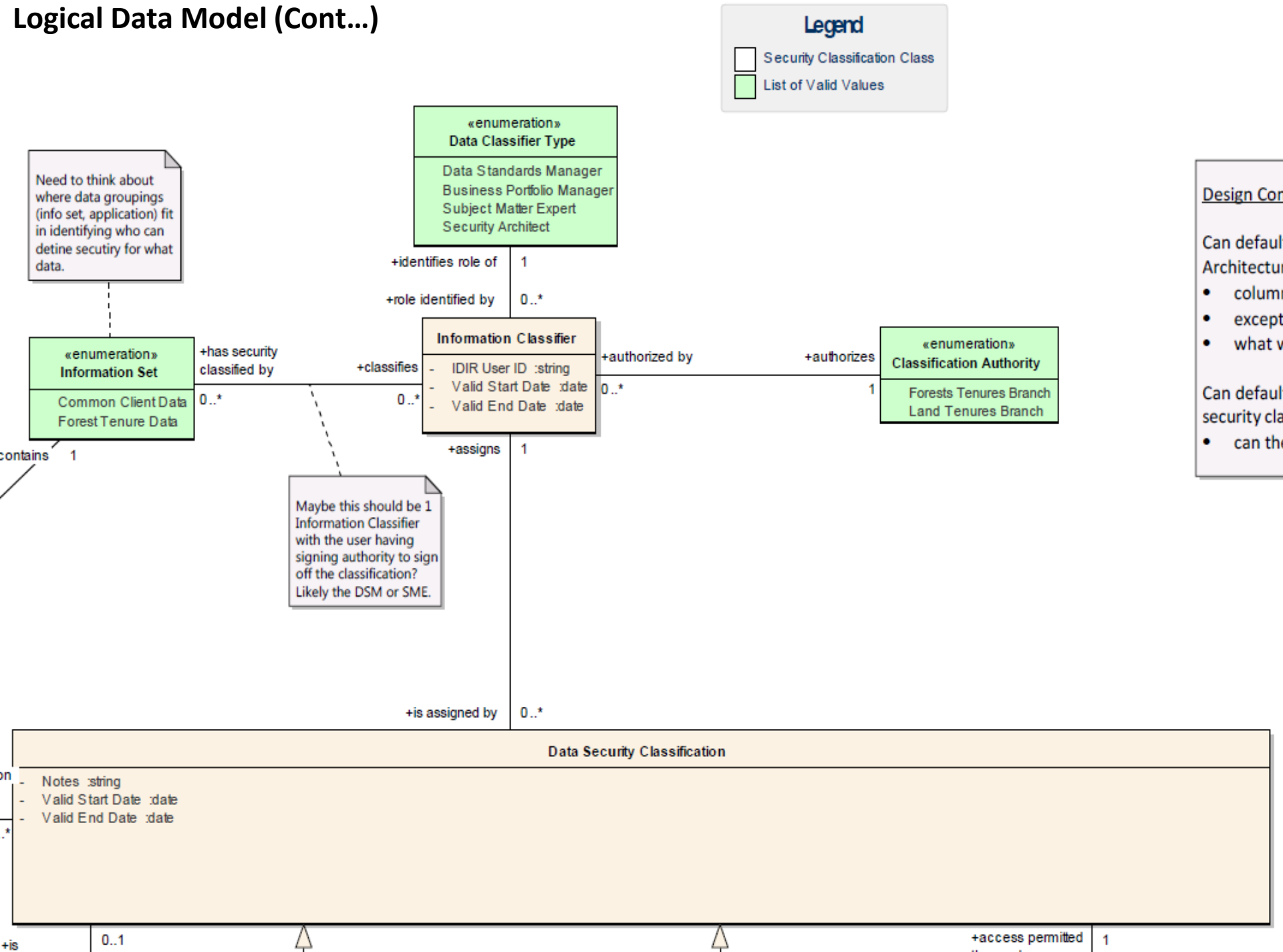
Logical Data Model



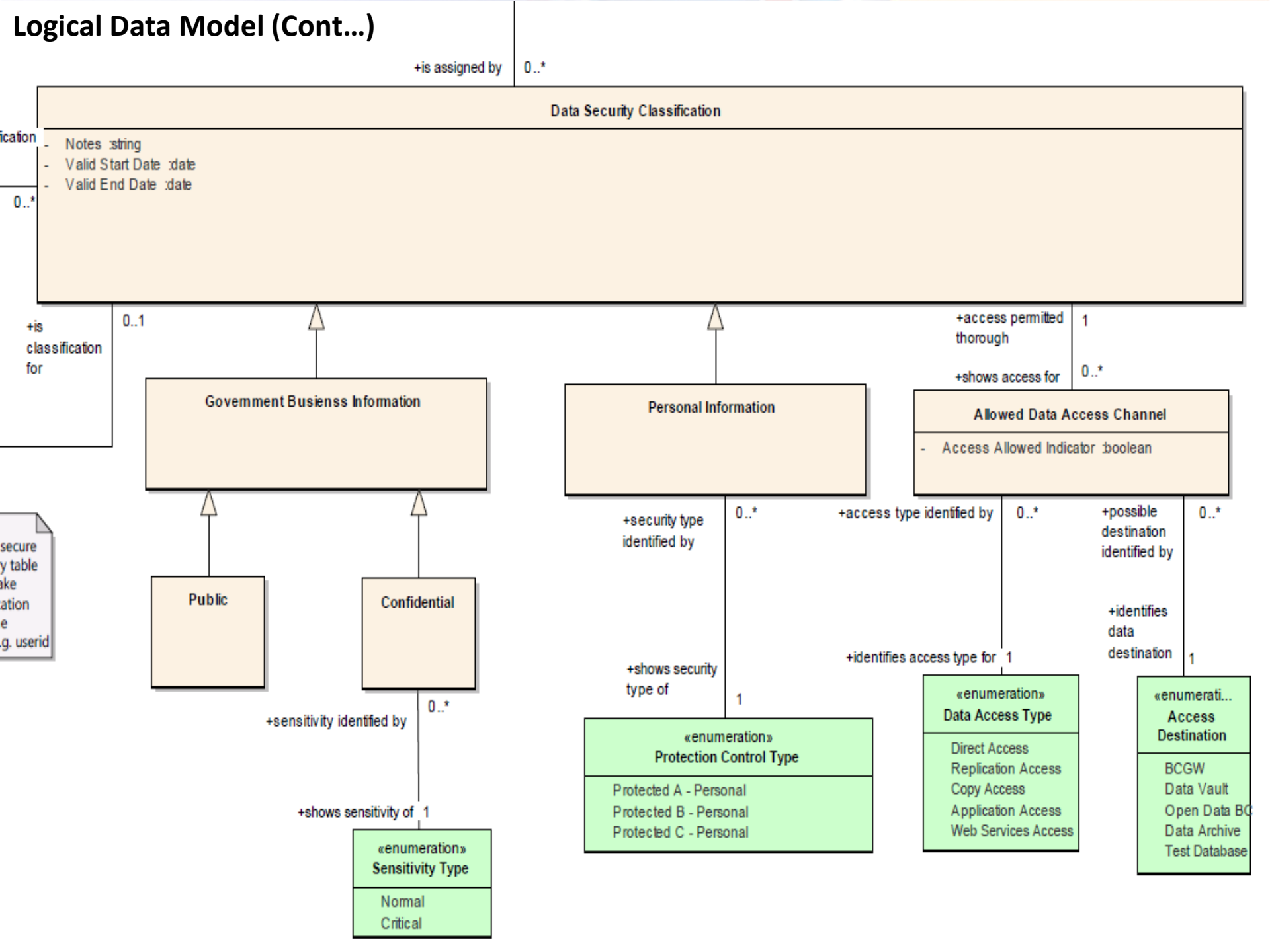


Logical Data Model (Cont…)

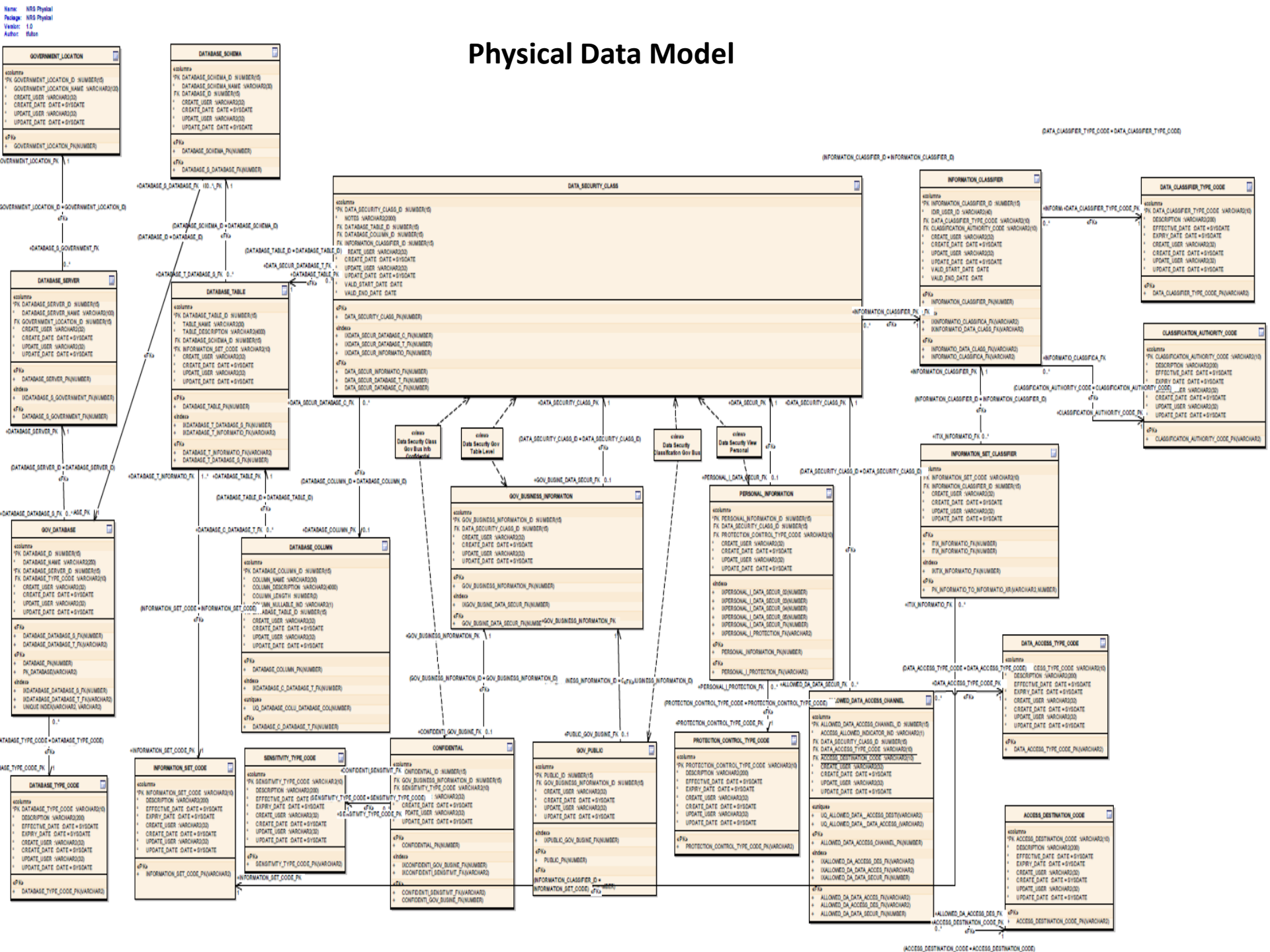
Logical Data Model (Cont…)



Logical Data Model (Cont…)



Physical Data Model



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?