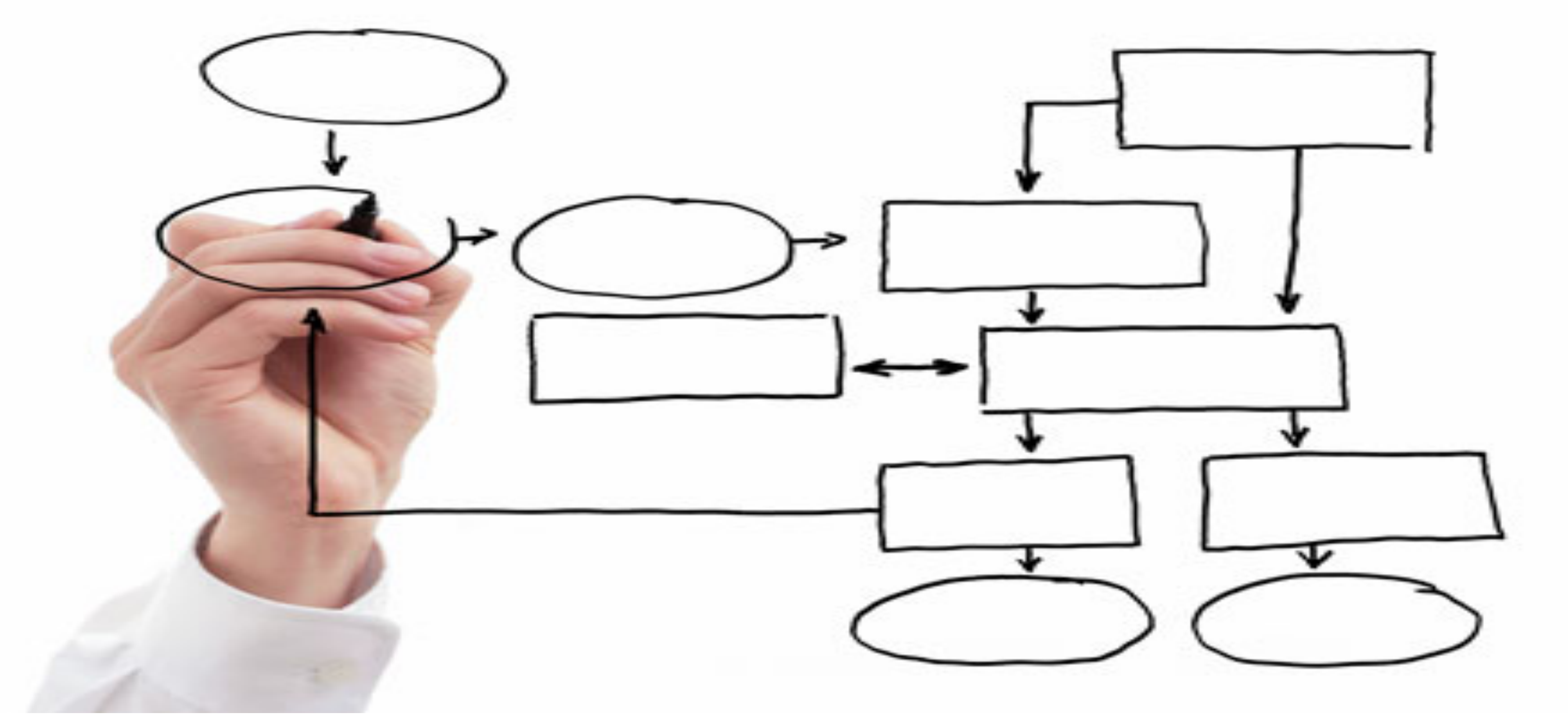


MIS 5121:Business Processes, ERP Systems & Controls

Week 12: Table Security

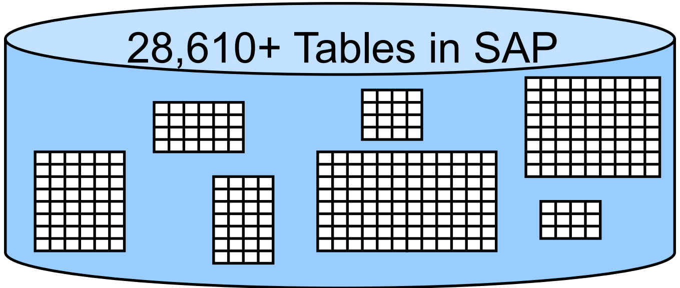
Edward Beaver
Edward.Beaver@temple.edu
ff

Key Information Technology Risks

- System Security
- Information Security Administration
- Data Migration
- Data Interface
- Instance Profile Security
- Change Management
- Transport Security
- **Table Security**
- Data Dictionary, Program and Development Security
- Logs and Traces
- Firefighter access
- Powerful User ID’s and Profiles
- Background Processing (Batch vs. foreground: real-time)

Table Security

- Tables are Integral part of SAP Application
  - Different Types of Tables to store the Data
    - System Tables (T000 – Clients, TDDAT – Table Authorization groups, USOBT_C – PFCG Transactions and Auth Objects)
    - Configuration / Control (T001 – Company codes, T001W – Plant Codes, TVAK – Sales Document Types)
    - Master Data (MARA – Material Codes, KNA1 – Customer Master: General)
    - Transaction Data (VBAK – Sales Doc Header, VBAP – Sales Doc Line Item, EKKO – Purchasing Doc Header)
  - Client-dependent and Client-independent



SAP: Table Driven System Execution

- SAP Processing is customized using thousands of **Configuration tables**
  - Access via the ‘Implementation Guide’ (Transaction SPRO)
  - Entries determine how transactions are processed
  - Entries also support implementation of controls (e.g. processing parameters and limits)

- ERP Systems are Dynamic
  - Configuration table values and therefore system processing, are continually changed (process changes, business structure, etc.
  - Effective processing and control Requires:
    - Managed Design
    - Documentation

Table Security

- Control Concerns
  - Access to maintain / modify table entries
  - Authorization group assignment (esp. custom tables)
  - Logging of changes (certain critical tables only) – next section

Risk and Recommendation
Table Security

Risks:

- Many tables (e.g. config) control how programs function. Changing them equivalent to changing a program
- Direct table changes bypass security, coded edit checks. High potential for corrupt data and compromise 'un-alterability'. Changes to client-independent tables could have unexpected side affects (affects all clients).
- Users with update access to table entries can modify customized tables not assigned to specific authorization group

Recommendations:

- Changes to configuration tables, table structures and certain system table entries should be made in DEV, tested in QA and migrated to PRD per change management process
- Direct access to maintain tables restricted to very few individuals
- Assure &SAP_EDIT backdoor change access in SE16N is Deactivated
- All critical tables assigned to an Authorization Group to prevent users not part of that group from accessing them (even for 'display' only)

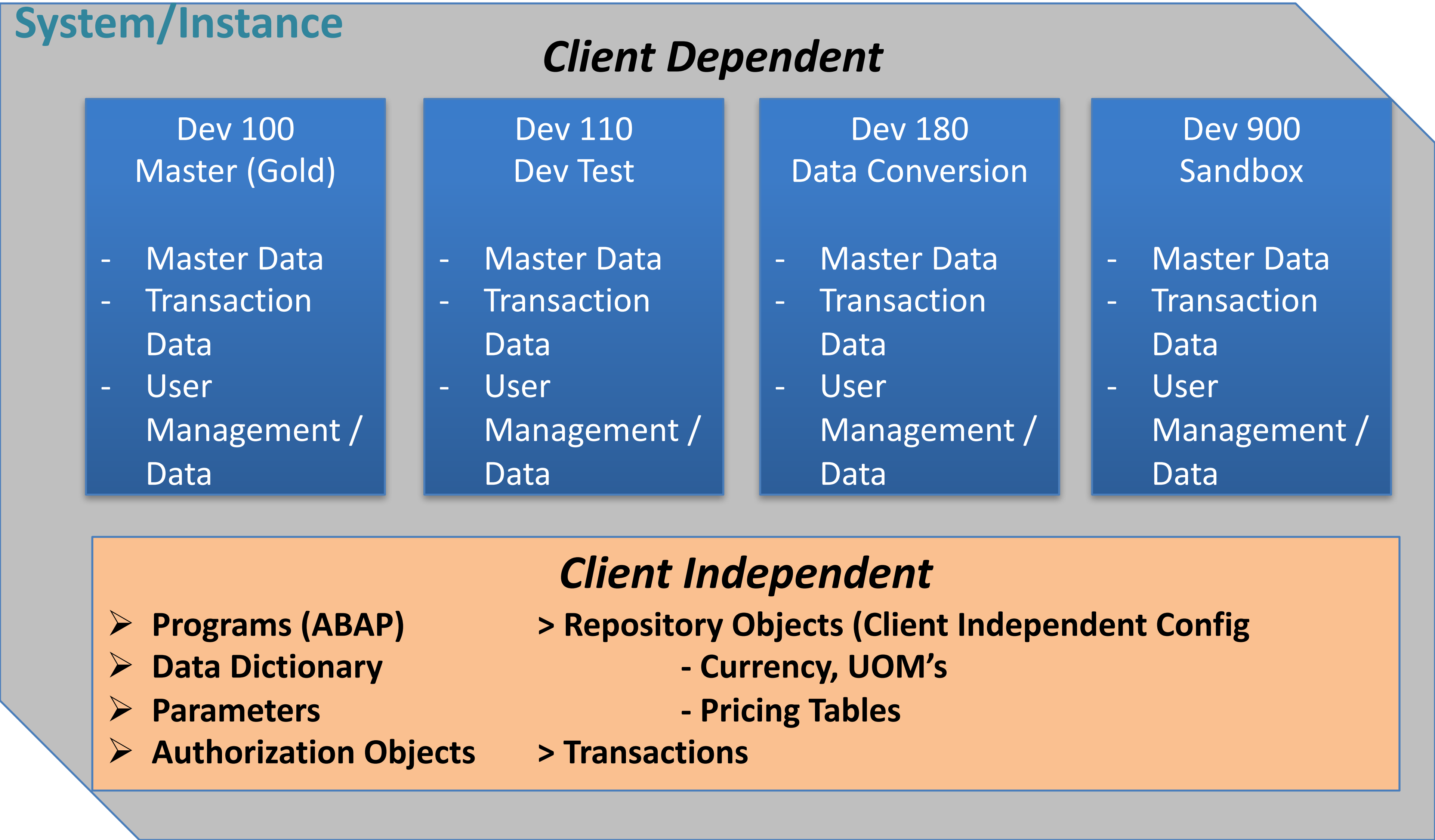
Key IT Controls Overview

- Table Security
  - 2-3 risks that exist
  - Common control recommendations for each

Extra Slides

System and Integration Controls

Client Dependent vs. Independent



System/Instance

Client Dependent

Dev 100
Master (Gold)

- Master Data
- Transaction Data
- User Management / Data

Dev 110
Dev Test

- Master Data
- Transaction Data
- User Management / Data

Dev 180
Data Conversion

- Master Data
- Transaction Data
- User Management / Data

Dev 900
Sandbox

- Master Data
- Transaction Data
- User Management / Data

Client Independent

- **Programs (ABAP)**
- **Data Dictionary**
- **Parameters**
- **Authorization Objects**

> Repository Objects (Client Independent Config
- Currency, UOM's
- Pricing Tables
> Transactions