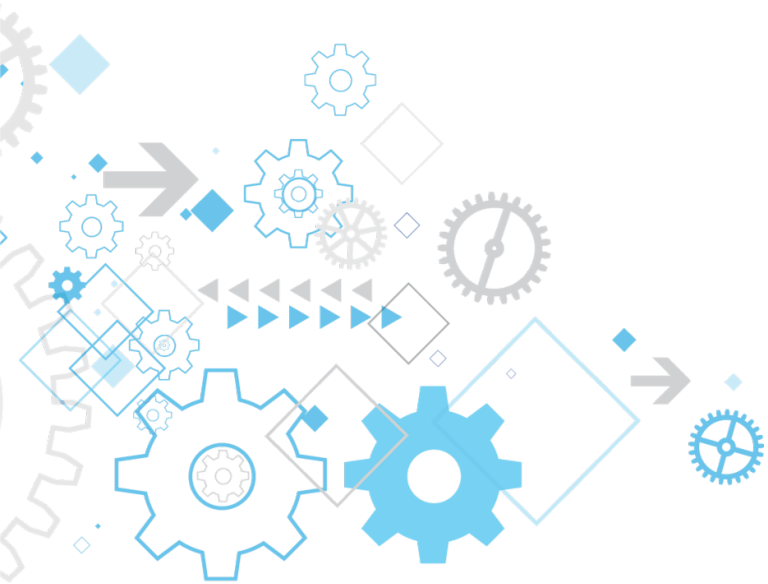


Session 60

Presenter – Frans Pelser

DB Audits / POPI / Data Quality Audits

DISCLAIMER

This presentation is only a summary of some of Adapt IT's products, features and their latest developments.

Adapt IT only intends for the information to give you an overview, and not a complete and comprehensive statement that necessarily suits your purposes.

Adapt IT reserves the right to change any information contained in this presentation and is not responsible for any loss that results from inaccuracies in the information.

You may not distribute or reproduce the information without Adapt IT's written permission.

Agenda

POPI and GDPR

- Background and importance for ITS Integrator clients
- Available Toolset
- Considerations

Database Security Audits

- Problem statement
- Application vs Database
- Appropriate Safeguards
- Typical Audit Findings

Value Add’s

- Data Quality Audit Services
- Data Categorization
- Recordkeeping of Custom Database Objects

POPI and GDPR: Background

- What is it about
  - Information on individuals and individual entities
  - Protecting the rights of individuals and individual entities related to their personal information
  - How organizations deal with the information

- References
  - GDPR: (EU) General Data Protection Regulation
    - https://gdpr.eu
  - POPI: (South African) Protection of Personal Information Act, 2013
    - https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

- One of the main functions of ITS Integrator is to maintain the records of Higher- and Further Education institutions. Many of these are of a highly personal nature and concerns the present and past students and staff members.

- Adapt IT list of items 

Available Toolset (1)

- User Access and Privileges
  - Granular / Applied per Menu Option
  - Engage Adapt IT PO's if
    - Additional Screens with less information

- Data Access / Restrictions
  - Integrator (Back-Office) Users limited e.g. to a single Campus / Department / Cost Centre
    - Applied to the appropriate set of options for each use case
  - iEnablers
    - Lecturer access information of students in specific class
    - Student only see own information
  - Engage Adapt IT PO's if
    - Tweaking is required

Available Toolset (2)

- User Authentication
  - Integrator Back-Office
    - Password Policy
  - iEnablers
    - Password in addition to PIN available, Outsourced Authentication through e.g. Active Directory being researched

- Access to the Jaspersoft Server Ad Hoc Reporting Tool
  - Administration required
    - Login Credentials for Individual Users
    - Set-ups for Access and Restrictions for Individual Users

Considerations (1)

- Consent
  - Applications Wizard / Registration “Rules and Regulations”
  - Personnel: How Handled for permanently appointed staff ?

- Processing by Adapt IT on behalf of the Institution
  - Requested data updates / data loading from the back-end
  - Work done by Adapt IT Consultants

- How long will information be retained
  - Should Information be classified, and retention schedules be based on classification? – Engage the Adapt IT PO’s
    - E.g. Academic Records to be retained, but should Academic Application Information be retained once Selection and Registration processes were completed?
    - Personnel e-Recruitment and Web Appointment Records?
    - Statutory (Tax / HEMIS / TVETMIS) Records and Records kept for evidence purposes?

Considerations (2)

- Processing by Third Parties
  - NSFAS / Debt Collection Agencies / Other

- The use of the Test Environment
  - Can information be stolen from the test environment?
  - Is there a requirement for data anonymization on the test environment?
  - Data Anonymization Strategies and Techniques
    - Data Masking (Impossible to get original values back)
    - Pseudonymization (Replacement with fake identifiers and pseudonyms, impossible to get original values back)
    - Generalization
    - Data Swapping (Rearrange values to prevent identification)
    - Data Perturbation (Adding random noise)
    - Encryption (One-way encryption vs. Encryption Key to decrypt)
  - Anonymization vs Hiding Information in the UI vs Protecting the Database so that data is only visible through the UI.

Considerations (3)

- Security Safeguards
  - Data kept for evidence purposes
    - Removal of personal details of users could destroy audit/log information

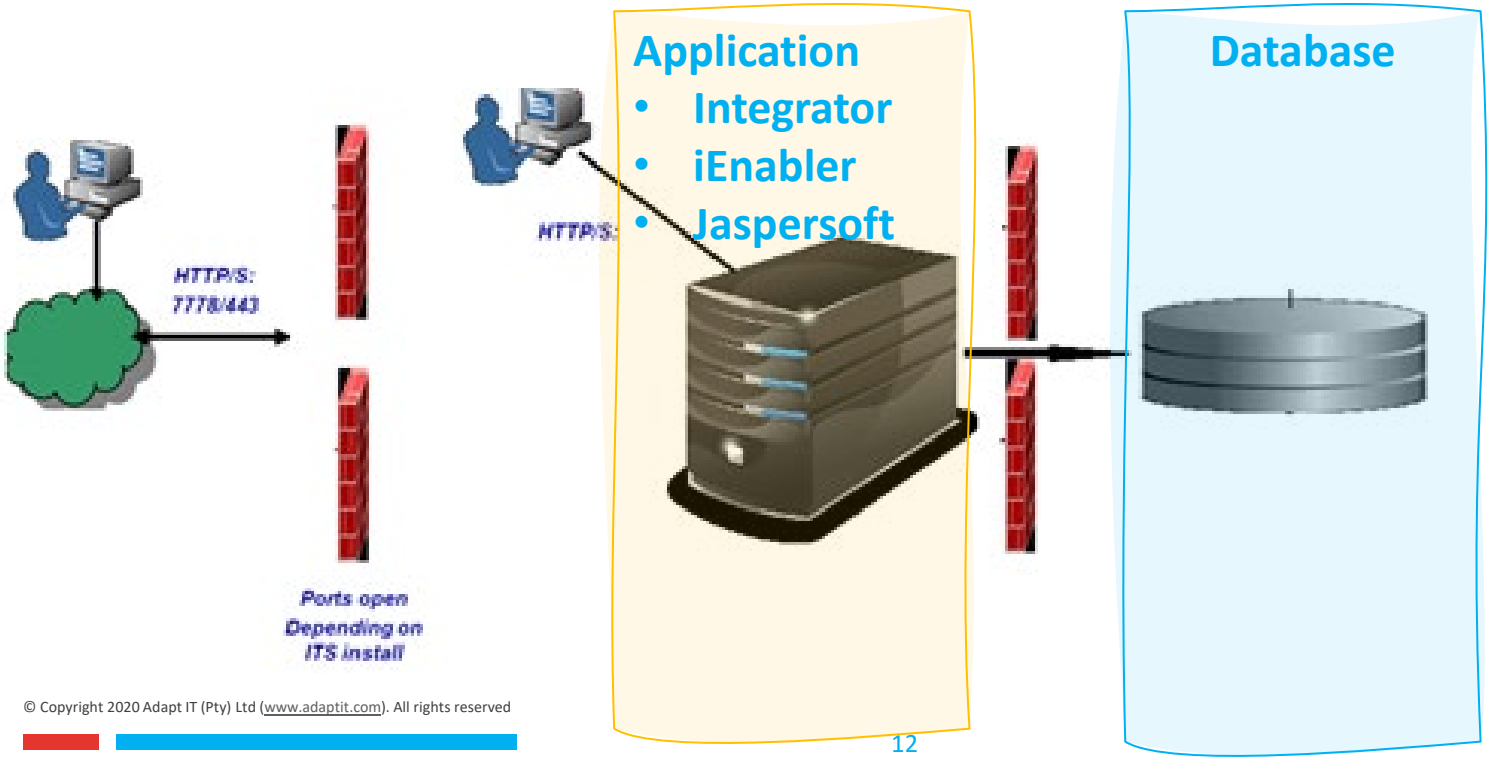
Risks

- Risks related to user behaviour
  - Sharing of credentials
  - Leaving Sessions open / System Inactive system logout
  - Storing or sharing of information outside Integrator / Emails
  - Forwarding Email Trails that contain information of a personal nature or login credentials
  - “Reply to all”
- Risks related to System Administrator behaviour
  - Control over authorisation (Who can see and do what) and Role Definition
    - Roles and Role definitions tend to be added, but not to be removed from users when they move to different positions
- Direct Database Access bypassing the application (ITS Integrator / iEnabler / Jaspersoft Server)
  - Authorised Access
  - Unauthorised back-end access

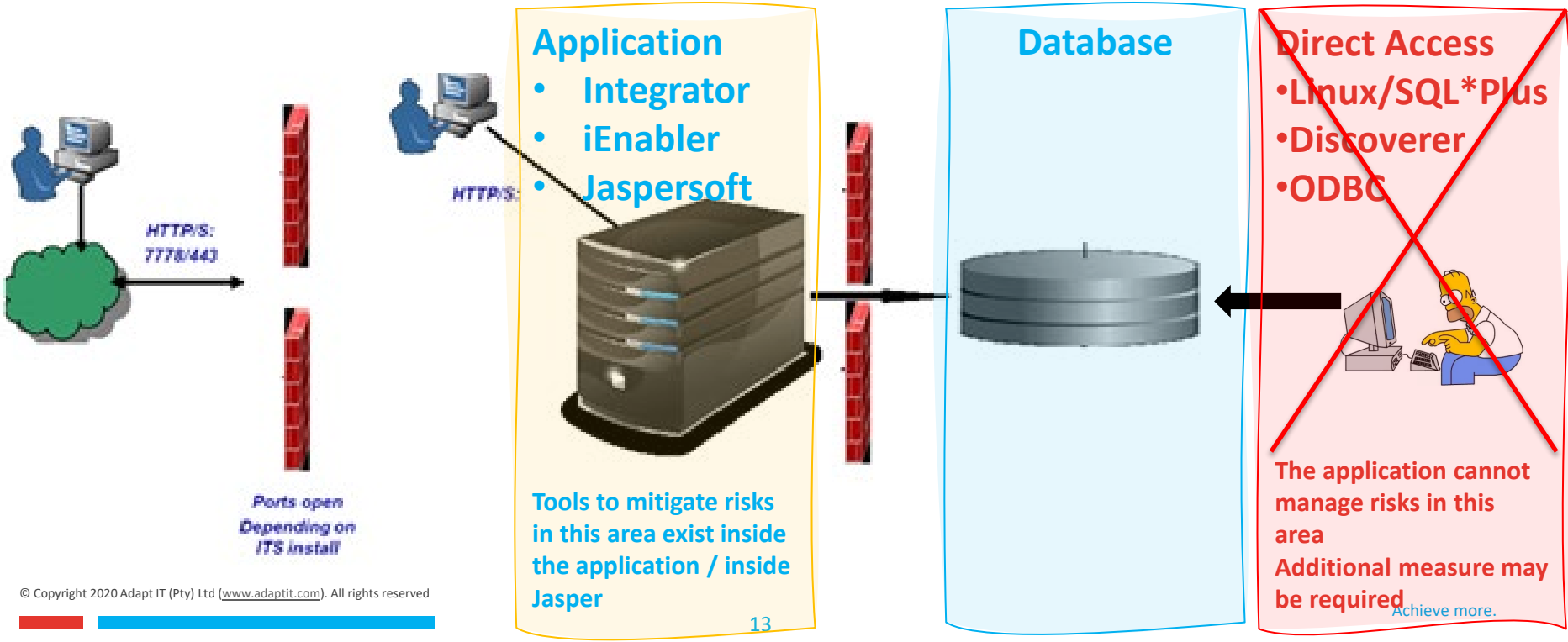
Database Security Audits

VS

Application vs Database: Recommended



Application vs Database: Risk Area



The appropriate solution for the situation

Integrator as hosted in the cloud

- Agreement with Adapt IT must cover all aspects

Integrator on Premise

- Agreement with Adapt IT
- Direct Access to the Database
- DBA Monitoring Contract
- Own Developers vs All Local Software outsourced to Adapt IT
- Log of changes when a new build is installed
- Audit log when Adapt IT technical staff log into the back-end
- Own DBA with system password: Responsibility for reviewing change logs

Typical Audit Findings

- Review of Audit Logs
  - Policy: Responsibility and Frequency
  - Evidence of Reviews
- Foreign Database Objects
  - Tables
  - What is it and who are using it / which applications are using it?
- Foreign Database Accounts (Users)
  - Who are using the accounts and what is the purpose of each account?
- Excessive Grants to the PUBLIC Role
  - Adapt IT can remove and replace with minimum required for Integrator
  - What will be the impact on custom software and own systems?
- Privileged SQL Statements
  - Who are using these:
    - The application (ITS Integrator) is not / Internal DBA's?

Typical Audit Findings: Audit Policies (1)

	Inside Integrator	Direct Access to DB
Password Policy	Back-Office (Rules in OID) iEnabler (Password in addition to PIN available, Outsourced Authentication through e.g. Active Directory being researched)	Not covered
Log of Failed Logins	Back-Office (Switch on and Monitor using EM iEnabler (New Functionality to lock / automatically unlock accounts with next Build, switch on with Process Event Code LW)	Not covered

Typical Audit Findings: Audit Policies (2)

	Inside Integrator	Direct Access to DB
Logs on changes to Master Data	Standard logs and Dynamic Logs	Direct Access is covered, but then, logs can be altered, purged from the back-end
Logs on Transactional Data		
Changes to Integrator configuration/set-up		
Changes to access	Standard Logs	The issue of Oracle Grant Statements to Oracle Accounts or Roles outside the ITS Integrator application is not logged

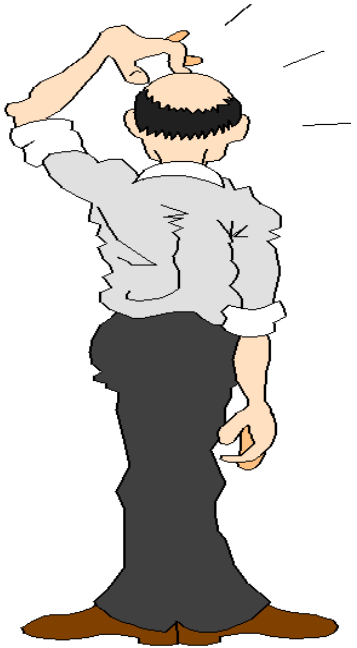
Typical Audit Findings: Audit Policies (3)

	Inside Integrator	Direct Access to DB
Users who change Posts / Roles	Standard Functionality – Refer {USERS-45 / 46}	Not Covered

Database Audits: Conclusion

- Risks related to the use of the application can be mitigated with existing tools; policies, procedures and contracts may have to be looked at
- Direct Access to the database may require additional tools, policies and procedures
  - Tools could be expensive

Data Quality Audit Services, Data Categorization and Recordkeeping of Custom Database Objects



Data Quality Audit Services

Problem Statement

- Different answers to the same question at different times
- Questions about reliability of information

Data Categorization

Use Cases

- Data categorization iro. POPI classification and reporting on volumes and movements of records
- Data anonymization in a Test or Query environment

Recordkeeping of Custom Database Objects

Problem Statement

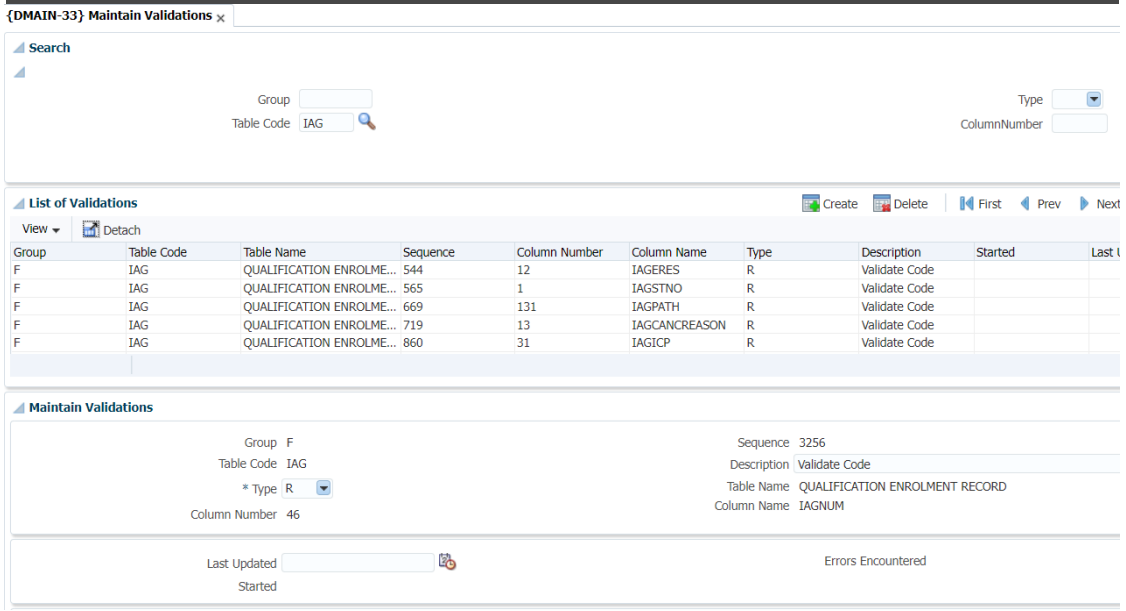
- No record or control of database tables created by institutional development staff
- Security Audit Findings

Data Quality Audit Service

Methodology

- Review DB Structure Against Documentation
- Validate data in database for missing reference information
- Set-up additional validation rules and include in validation.
- Steps to remedy existing gaps
- Steps to prevent future issues
- Set-up and monitoring of continuous validation runs

Set-up



Data Categorization

Data Category List / User Defined

{DMAIN-18} Data Category Codes

Data Category Codes {DMAIN-18} Create Delete

View Detach

* Category	Category Description
PI	Personnal Identifiers
NP	No POPI impact
SU	Structure / Set-up
NA	Names of Individuals
LS	Local Software
DS	Discontinued
S	System Default Records
LG	Log
SN	Sensitive Personal Information
RM	To be deleted when anonimized
BD	Bank Details
SE	Security Set-up
RP	Summarized Reporting Data
US	Unstructured
T	Temp Table
SA	Tax / Salary

Data Category Attached to Table

Maintain Tables

Table Code PAA
Table Sub Code PR1
Subsystem Code P
System Code P

Table Name PERSONNEL PERSONAL DETAIL
Description The table includes the biographical and work related detail
Subsystem Name
System Name

Storage Definition Code P01SPC
Log Table ID PEQ
Date Released 01-Jan-1986

Storage Definition Name
Log Table Name
Date Discontinued

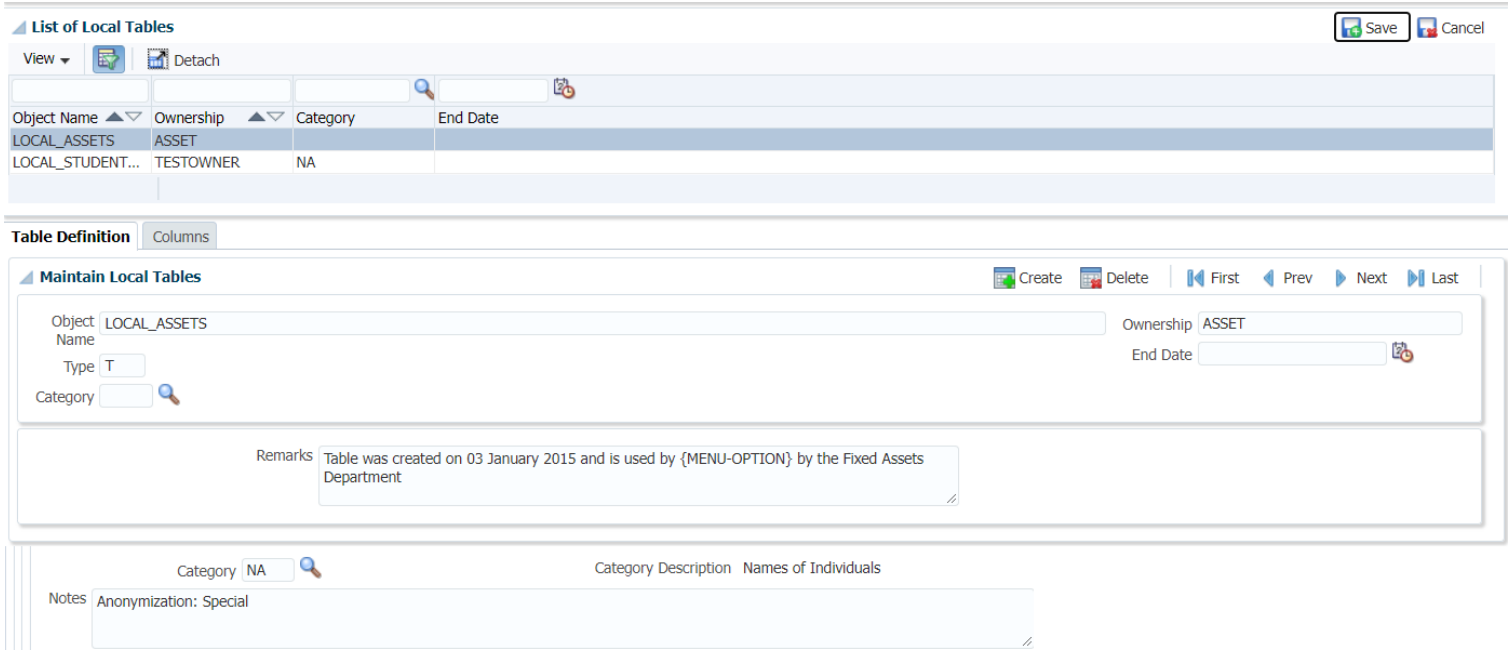
* On this Environment Y - Yes
* Incl in Data Model N - No
* Code Structure Table Y - Yes
Exclude ADF? N - No
Nr of Columns/Line 2

* Global Temp No
* Used in Data Scripts Y - Yes
Constraint Level 0
Task Code
Local Software ? N

Category NA
Category Description Names of Individuals

Notes Anonymization: Special

Recordkeeping of Custom Database Tables



Q & A

ENABLING OUR PEOPLE AND PARTNERS TO Achieve More.