VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Migrating DB2® Security to RACF®

Presented by
Vanguard Integrity Professionals

IBM Server Proven

Business Partner IBM

Legal Notice

Copyright

Trademarks

IBM, RACF, DB2, CICS, OS/390 and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Session Topics

- Benefits of Using RACF for DB2 Security
- Migrating from DB2 Security to RACF Security
  - – Migration Planning – Implementation Options
  - – Converting DB2 Grants to RACF profiles
  - – DB2 External Security Module for RACF
- Migration Considerations

Organizational Benefits of RACF for DB2

- Fundamental Security Principals
  - Accountability
  - Auditability
  - Separation of duties
  - Least privilege

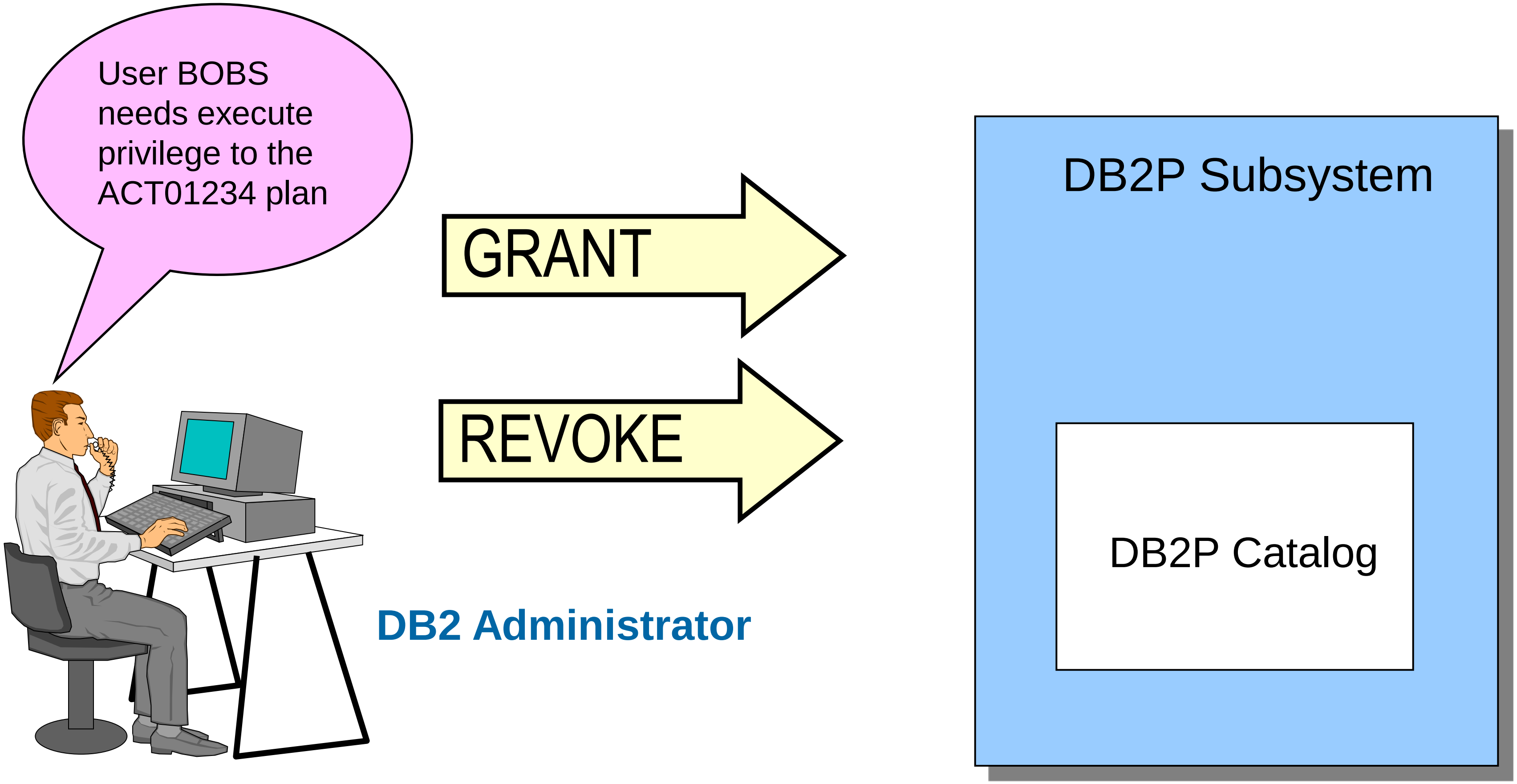
Organizational Benefits of RACF for DB2

- RACF is administered by staff focused on security.
- Database access is just one of the security areas on which they are focused.
- Using RACF encourages separation of duties between security administration and DB2 DBA role.
- RACF Security staff is aware of compliance considerations.
- Compliance reports from one source.

Technical Benefits Of RACF for DB2

- One or several sets of general resource classes
- A single profile can protect multiple objects via generics, RACFVARS, group class profiles
- Phased implementation by DB2 subsystem, object type, and object
- Support for IBM® z/OS® RACF constructs introduced in z/OS V1R10 and later releases, e.g. distributed identities
- Conversion utility available to assist RACF implementation
- Further Enhancements are likely

Traditional DB2 Security



User BOBS needs execute privilege to the ACT01234 plan

GRANT

REVOKE

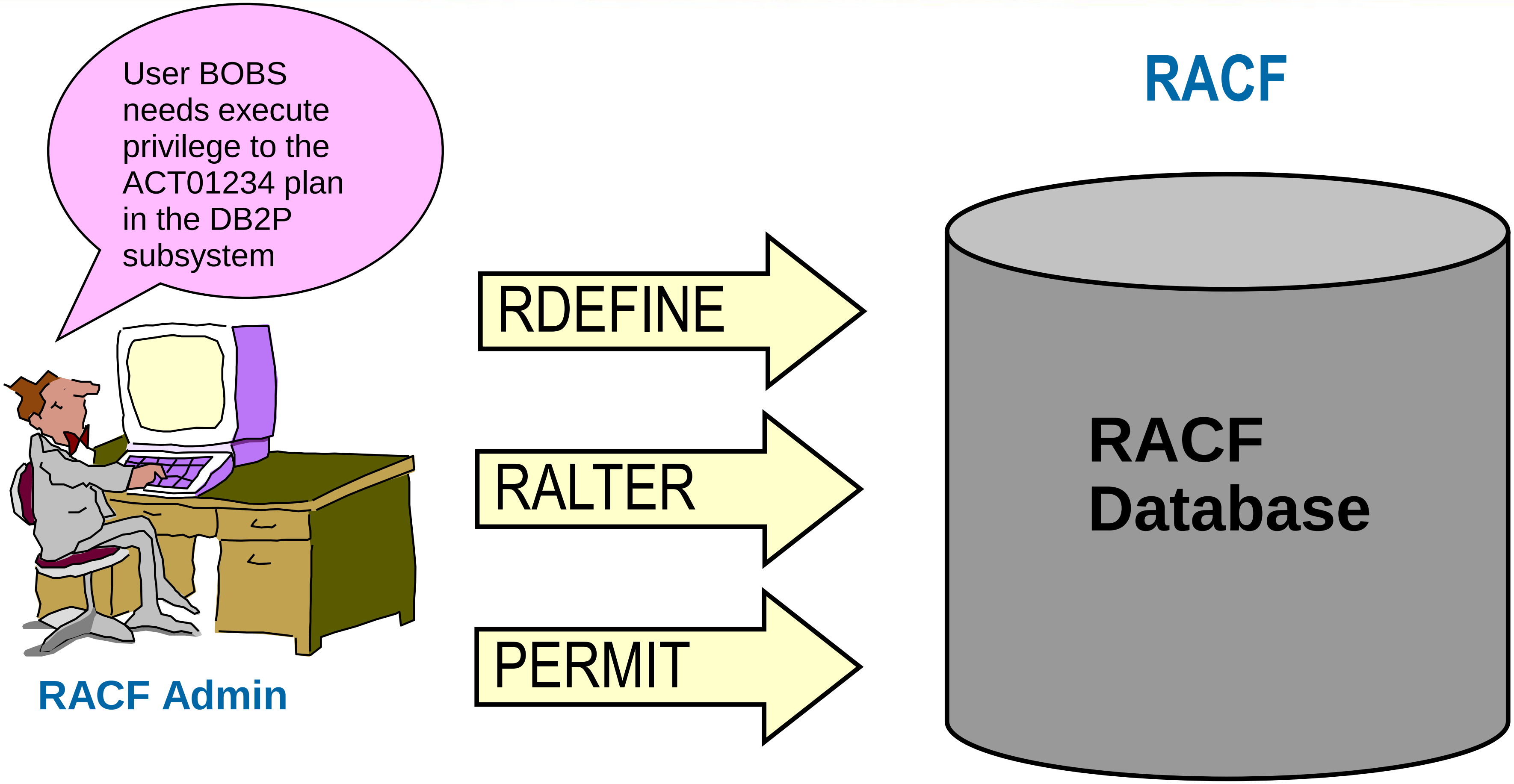
DB2 Administrator

DB2P Subsystem

DB2P Catalog

GRANT EXECUTE ON PLAN ACT01234 TO BOBS

RACF Security For DB2 Objects

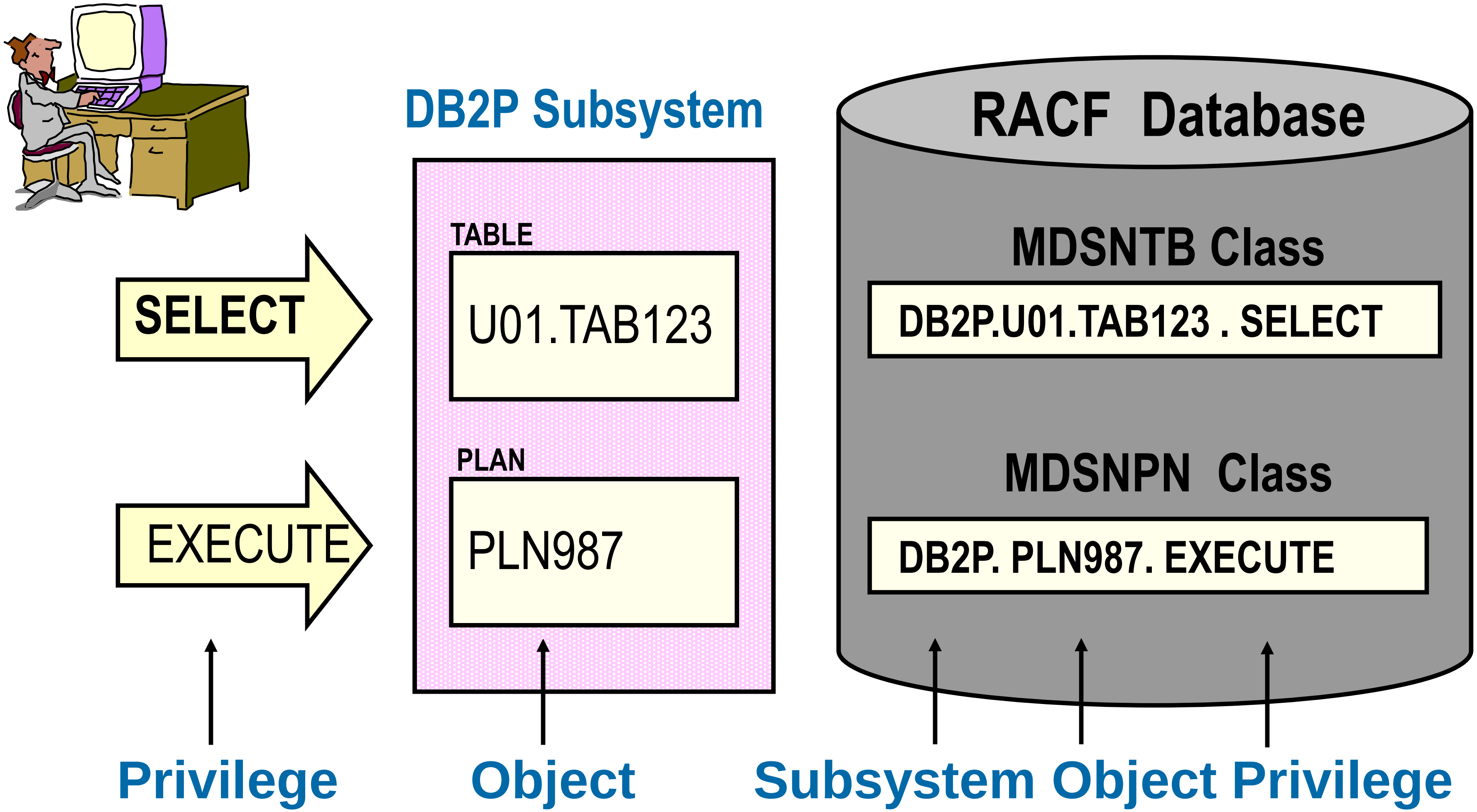

User BOBS needs execute privilege to the ACT01234 plan in the DB2P subsystem
RACF Admin
RDEFINE
RALTER
PERMIT
RACF
RACF Database

```
RDEF MDSNPN DB2P.ACT01234.EXECUTE OW(DB2ADM) UA(NONE)
PE DB2P.ACT01234.EXECUTE CLASS(MDSNPN) ID(BOBS) AC(READ)
```

RACF Classes For DB2 Objects

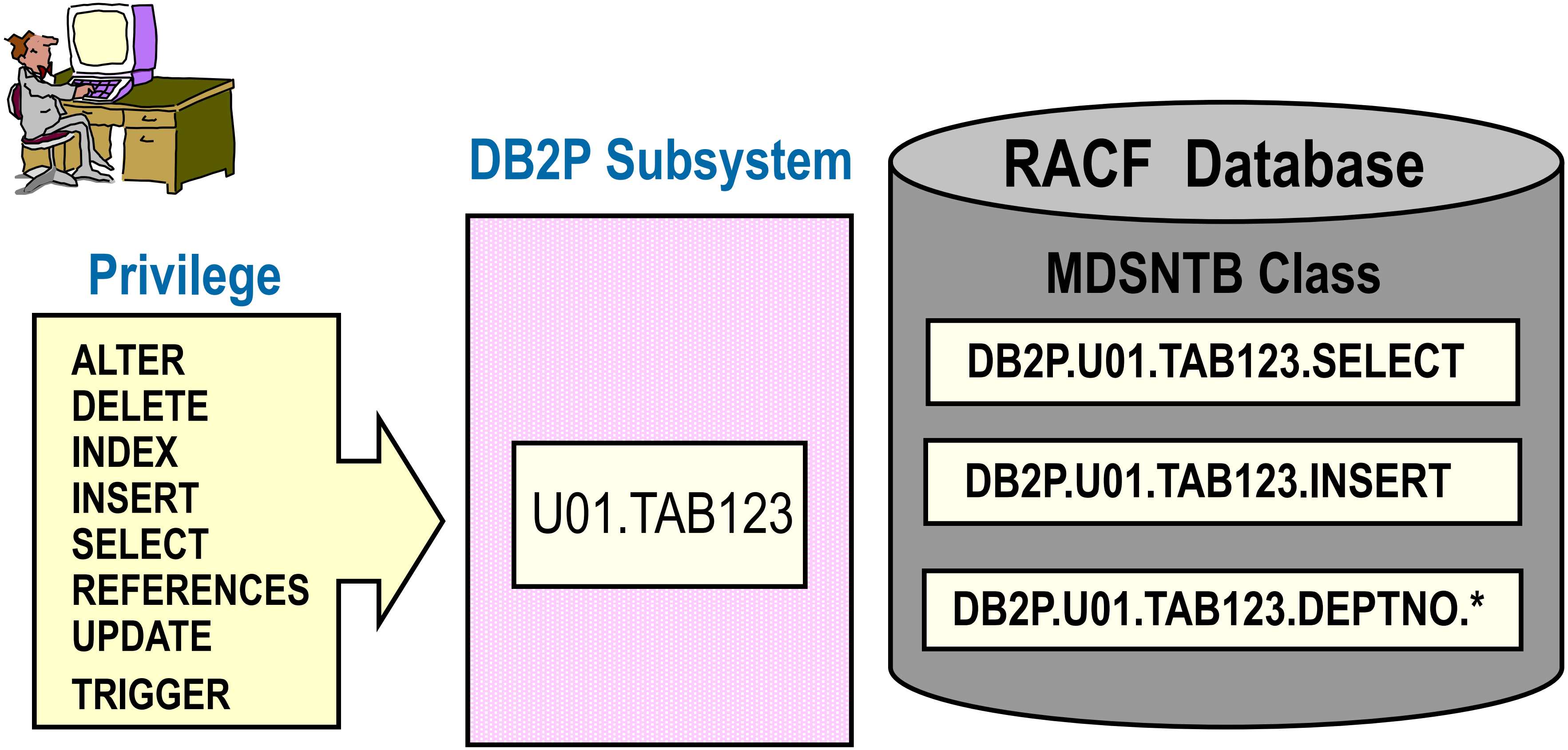
DB2 Object Type	Member	Grouping
Bufferpool	MDSNBP	GDSNBP
Collection	MDSNCL	GDSNCL
Database	MDSNDB	GDSNDB
JAR - Java Archive File	MDSNJR	GDSNJR
Package	MDSNPK	GDSNPK
Plan	MDSNPN	GDSNPN
Schema	MDSNSC	GDSNSC
Sequence	MDSNSQ	GDSNSQ
Storage Group	MDSNSG	GDSNSG
Stored Procedure	MDSNSP	GDSNSP
System	MDSNSM	GDSNSM
Table / Index / View	MDSNTB	GDSNTB
Table Space	MDSNTS	GDSNTS
User Defined Distinct Type	MDSNUT	GDSNUT
User Defined Function	MDSNUF	GDSNUF

RACF Profile Syntax For DB2 Objects



RACF Profiles for Tables

DB2-subsystem-name.owner.table-name.privilege
DB2-subsystem-name.owner.table-name.column-name.privilege



Privilege

- ALTER
- DELETE
- INDEX
- INSERT
- SELECT
- REFERENCES
- UPDATE
- TRIGGER

DB2P Subsystem

U01.TAB123

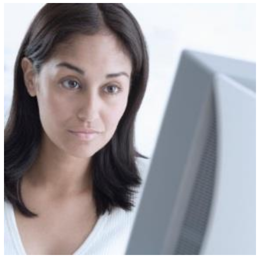
RACF Database

MDSNTB Class

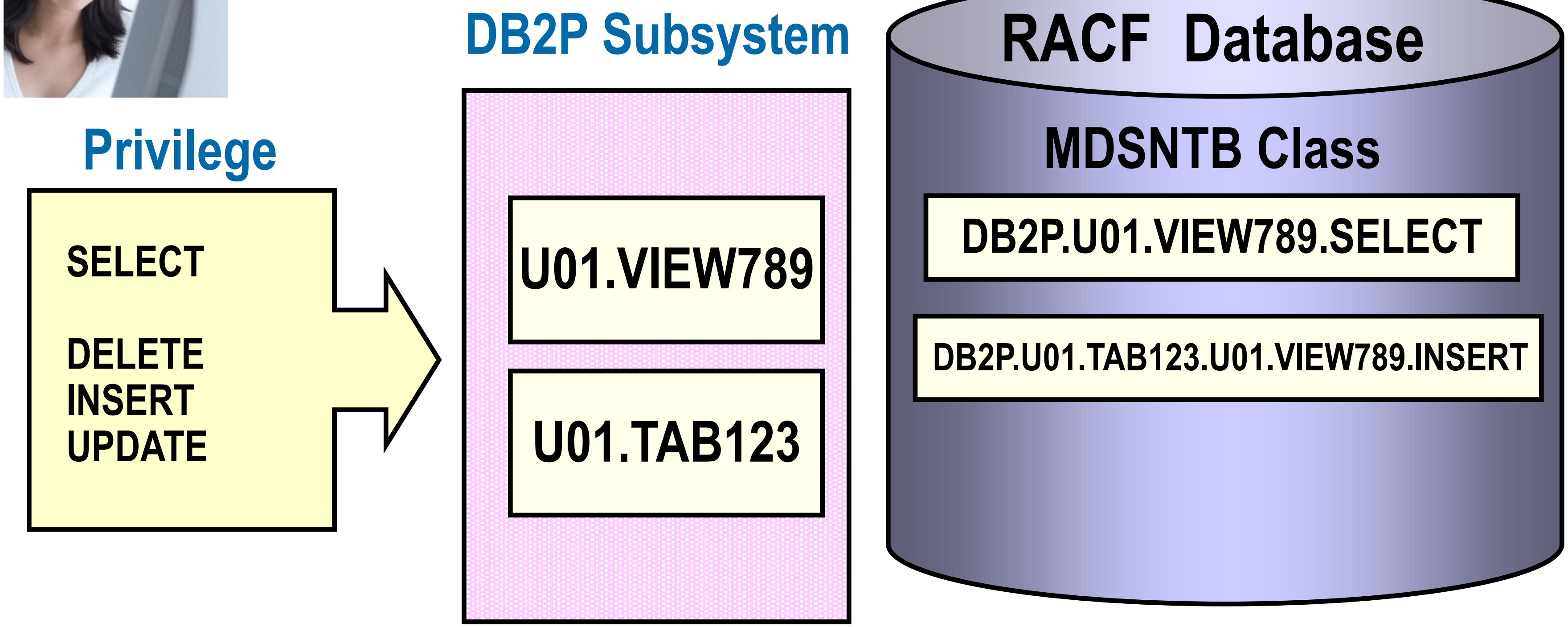
- DB2P.U01.TAB123.SELECT
- DB2P.U01.TAB123.INSERT
- DB2P.U01.TAB123.DEPTNO.*

Profiles for Views

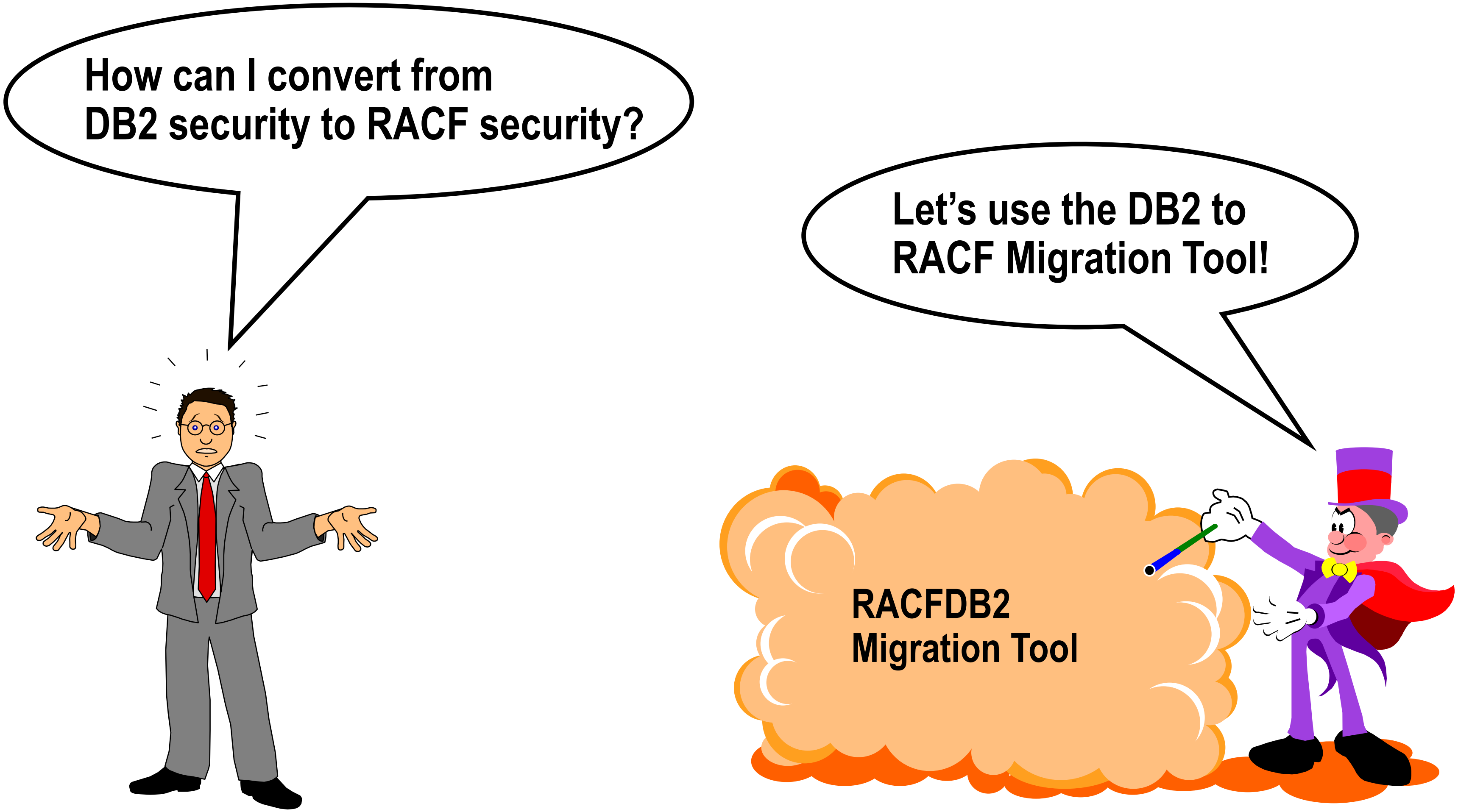
DB2-subsystem.owner.view.SELECT
DB2-subsystem.table-owner.table-name.view-owner.view-name. privilege



New Format introduced in DB2 V9 via PTF UK50217



Migrating from DB2 to RACF Security



DB2 to RACF Migration Planning

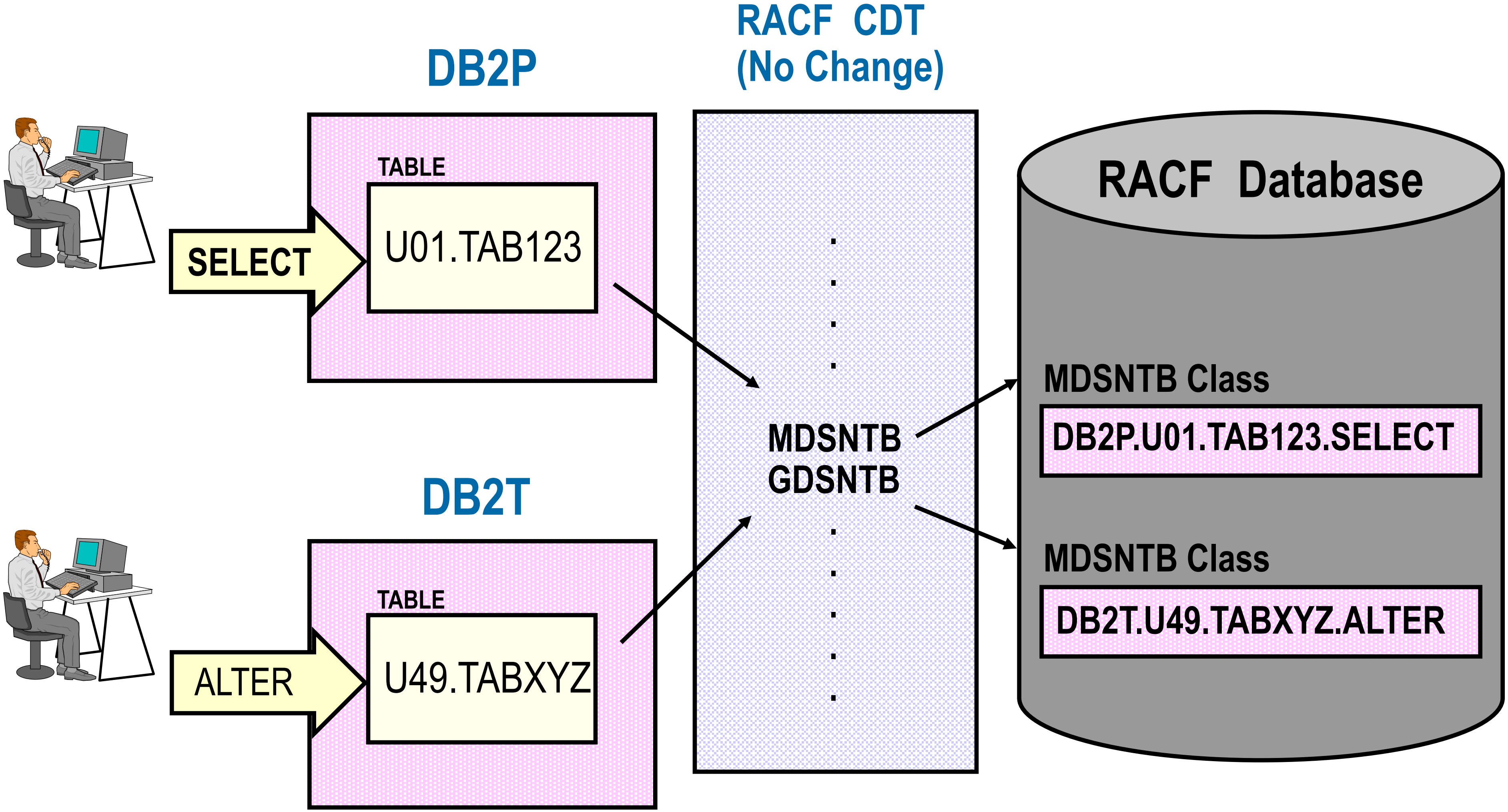
- Is the current “internal” DB2 security in “good enough shape” to consider converting to RACF?
- Where can I find a conversion tool?
  IBM website – RACF Downloads Page
  - http://www-03.ibm.com/systems/z/os/zos/features/racf/goodies.html
  - Tool developed for DB2 V6 (1999) for OS/390® & V7 for z/OS (2001)
- What structure in RACF should be my target?
  - Multi-Subsystem Scope Classes vs.
    Single Subsystem Scope Classes?

Single or Multi-subsystem Scope?

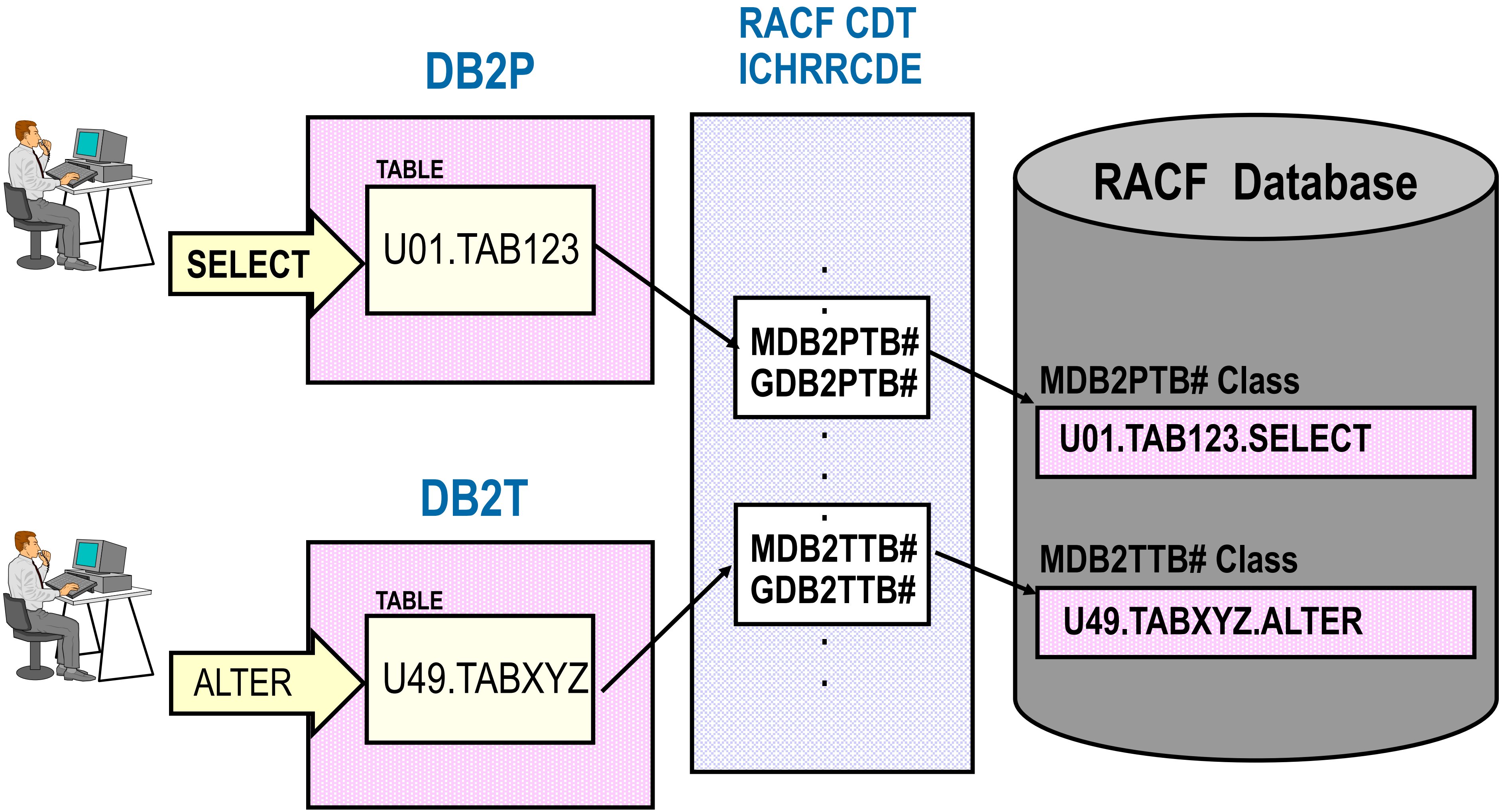
- Multi-Subsystem Scope Classes - Default
  - First profile qualifier is DB2 subsystem name
  - Resource Classes are predefined
  - Delegation of administrative authority by DB2 subsystem requires CLAUTH and Genericowner

- Single Subsystem Scope Classes - Optional
  - DB2 subsystem name not in profile
  - DB2 subsystem name is part of the class name
  - Requires definitions to be added to CDT class
  - Delegation of administrative authority by DB2 subsystem requires only CLAUTH

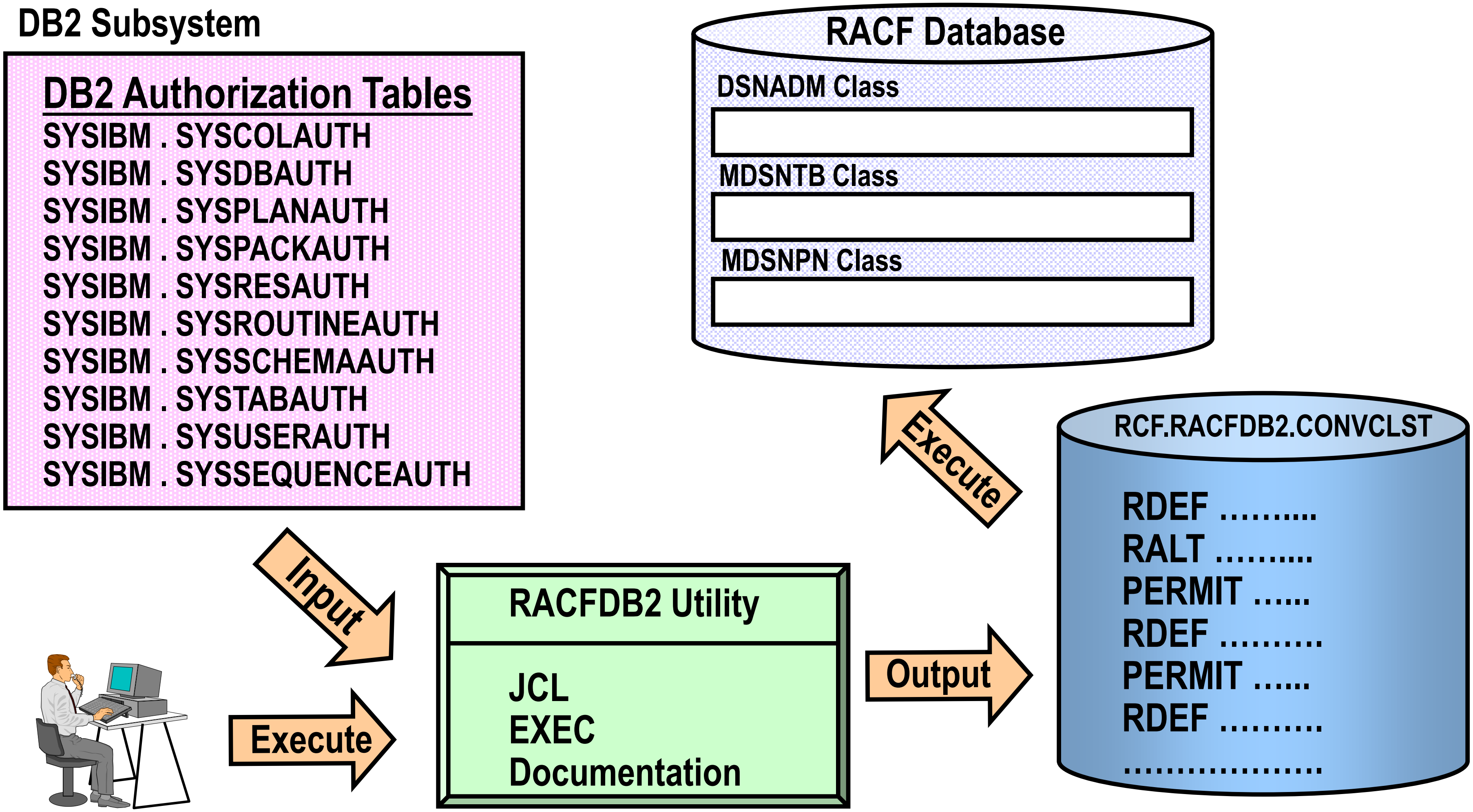
Multi-Subsystem Scope (Default)



Single-Subsystem Scope



DB2 to RACF Migration Tool



DB2 Subsystem

DB2 Authorization Tables

SYSIBM . SYSCOLAUTH
SYSIBM . SYSDBAUTH
SYSIBM . SYSPLANAUTH
SYSIBM . SYSPACKAUTH
SYSIBM . SYSRESAUTH
SYSIBM . SYSROUTINEAUTH
SYSIBM . SYSSCHEMAAUTH
SYSIBM . SYSTABAUTH
SYSIBM . SYSUSERAUTH
SYSIBM . SYSSEQUENCEAUTH

RACF Database

DSNADM Class

MDSNTB Class

MDSNPN Class

Input

Execute

RACFDB2 Utility

JCL
EXEC
Documentation

Output

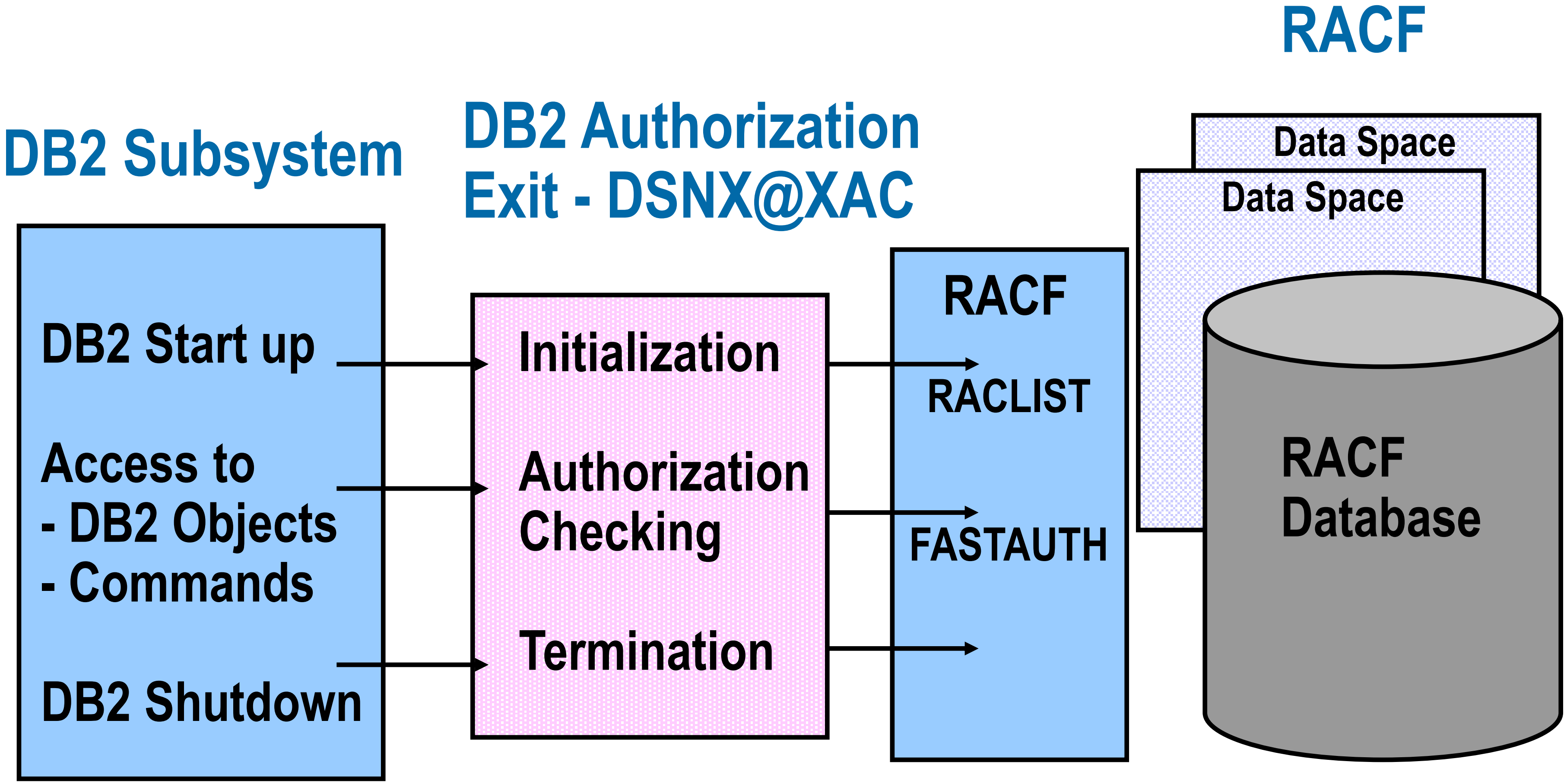
Execute

RCF.RACFDB2.CONVCLST

RDEF ....
RALT ....
PERMIT ......
RDEF ....
PERMIT ......
RDEF ....
....

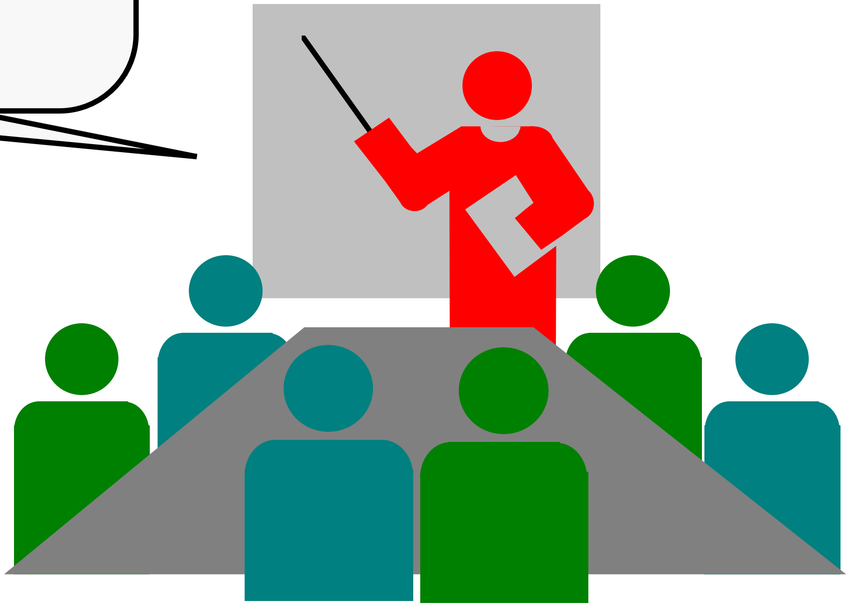
DSNX@XAC DB2 Authorization Exit

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

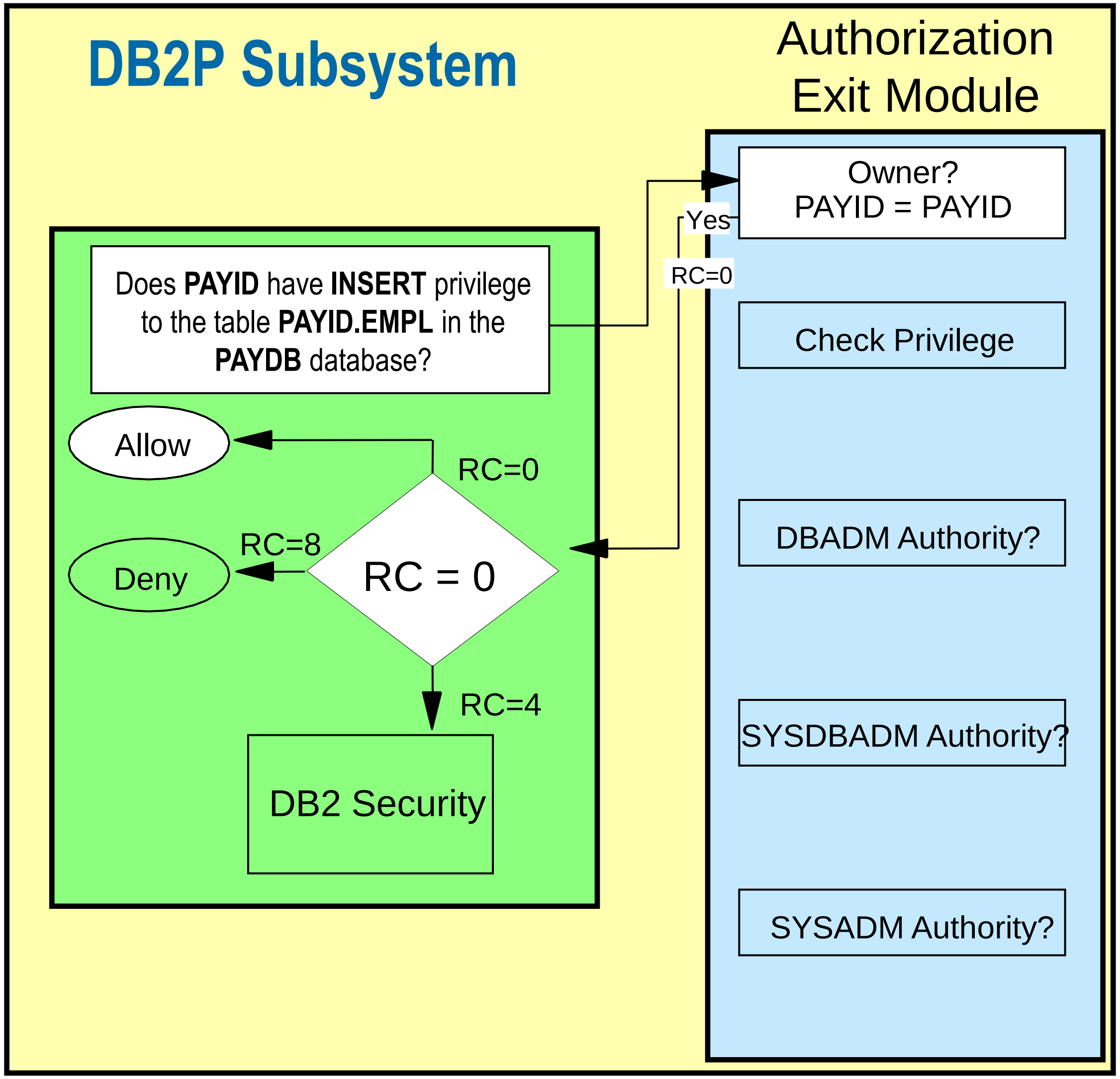


Access Control With RACF

To access a DB2 Object requires:
Ownership
or
Privilege to Object
or
DB2 Administrative Authority



Access Allowed By Ownership



DB2P Subsystem

Authorization Exit Module

Does **PAYID** have **INSERT** privilege to the table **PAYID.EMPL** in the **PAYDB** database?

Owner?
PAYID = PAYID

Yes

RC=0

Check Privilege

DBADM Authority?

SYSDBADM Authority?

SYSADM Authority?

RC = 0

RC=0

Allow

RC=8

Deny

RC=4

DB2 Security

RACF

Data Space

MDSNTB Class

DB2P.PAYID.EMPL.INSERT
UA(NONE) PHILE(READ)

DSNADM Class

DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

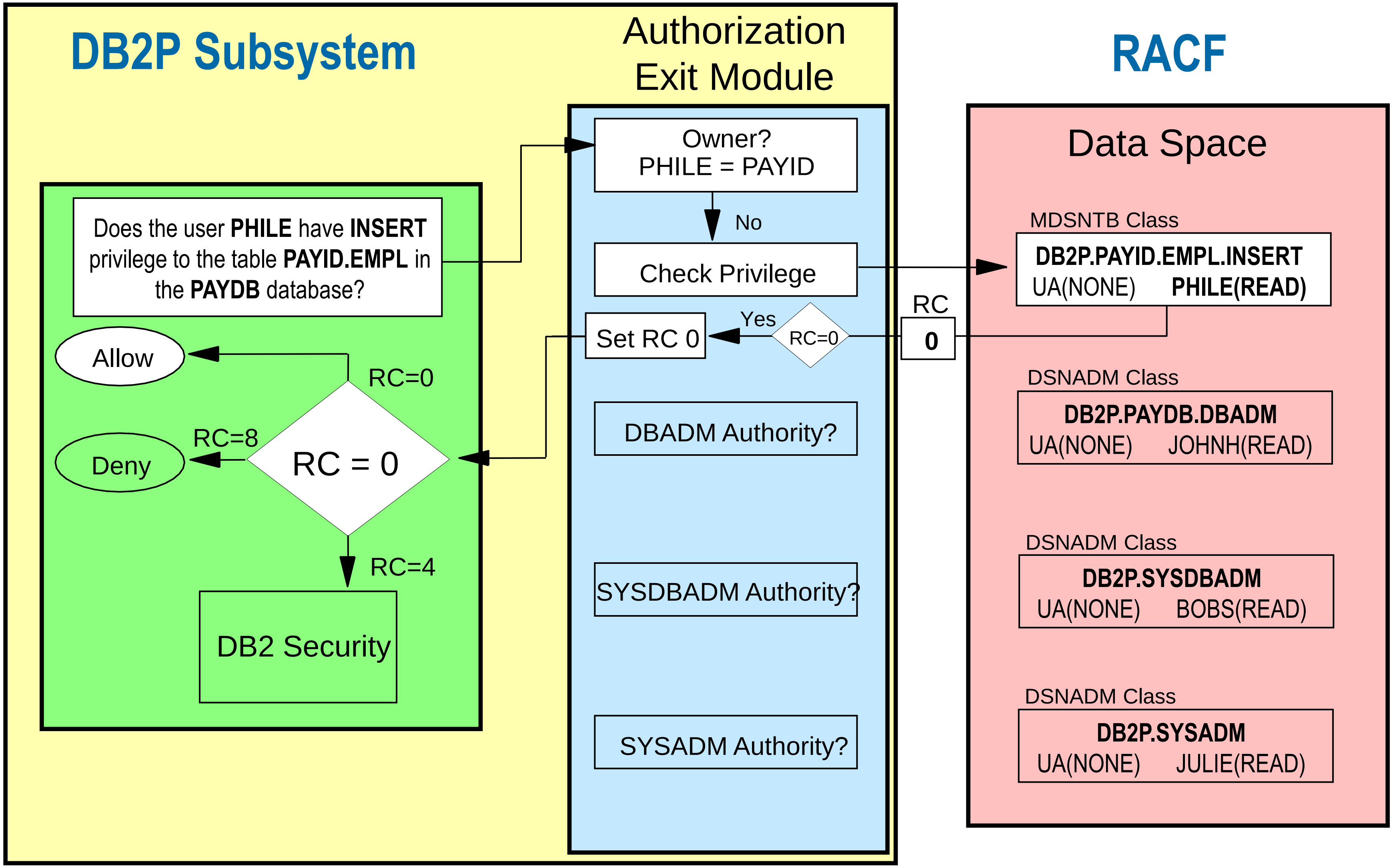
DSNADM Class

DB2P.SYSDBADM
UA(NONE) BOBS(READ)

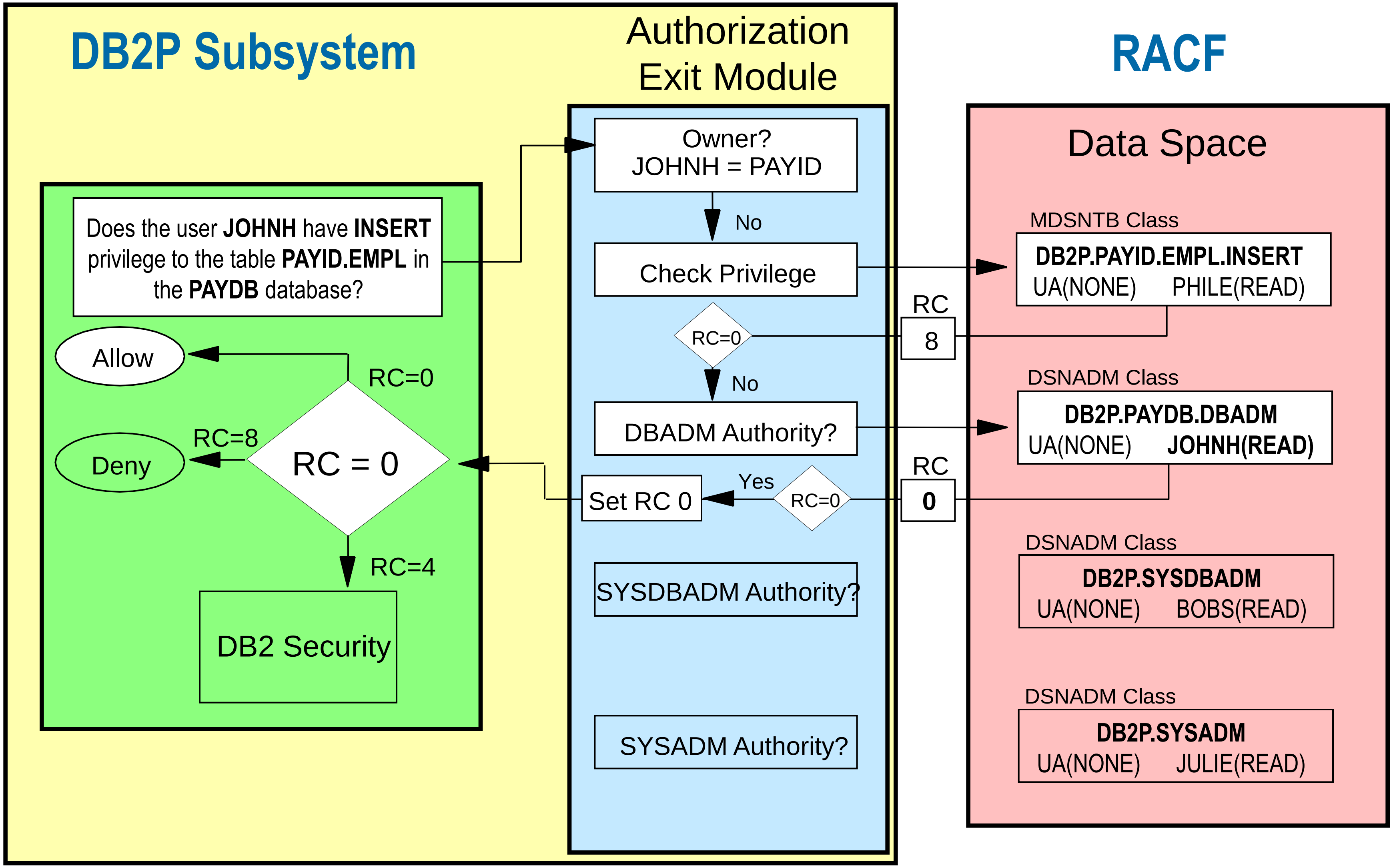
DSNADM Class

DB2P.SYSADM
UA(NONE) JULIE(READ)

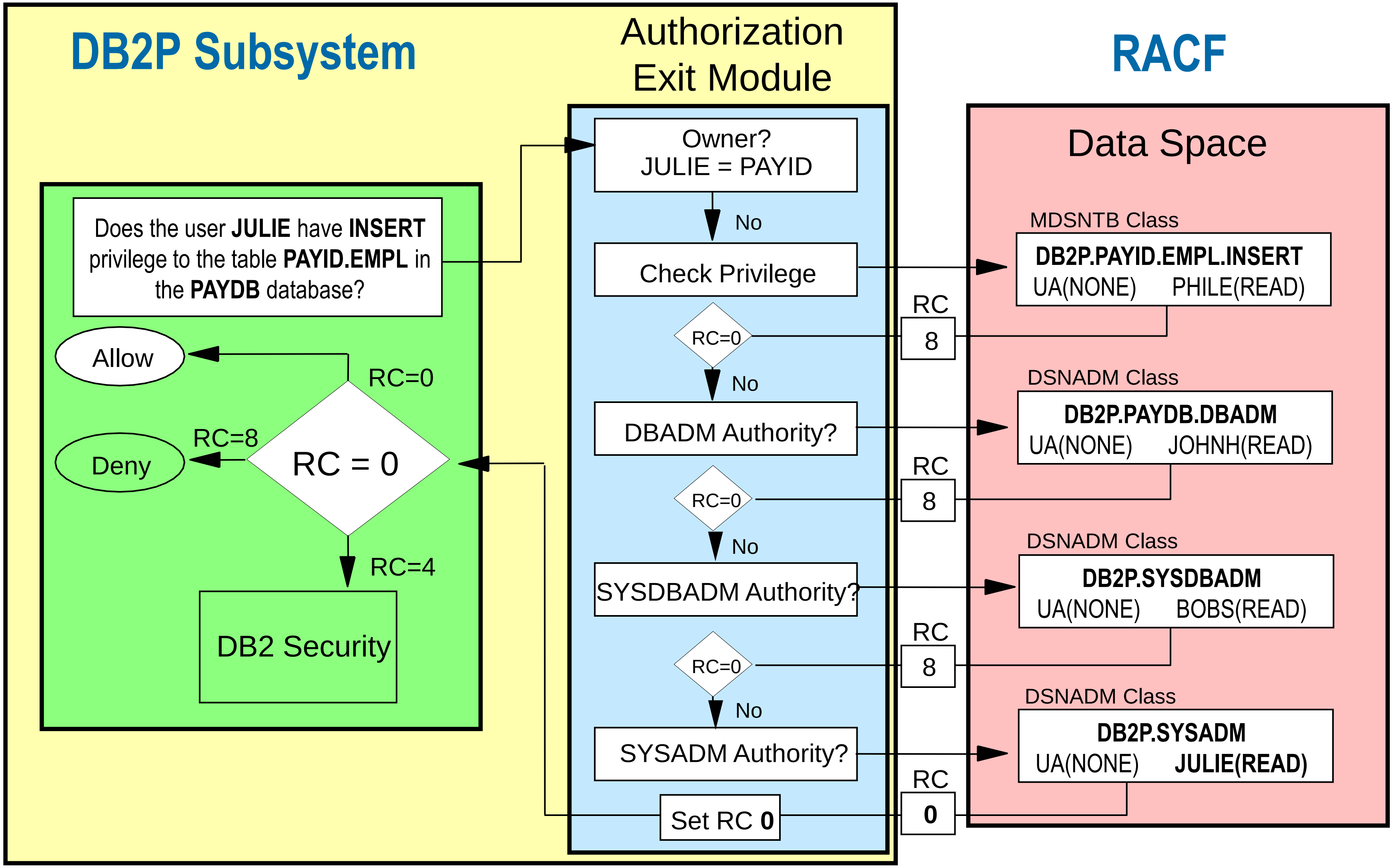
Access Allowed By Object Profile



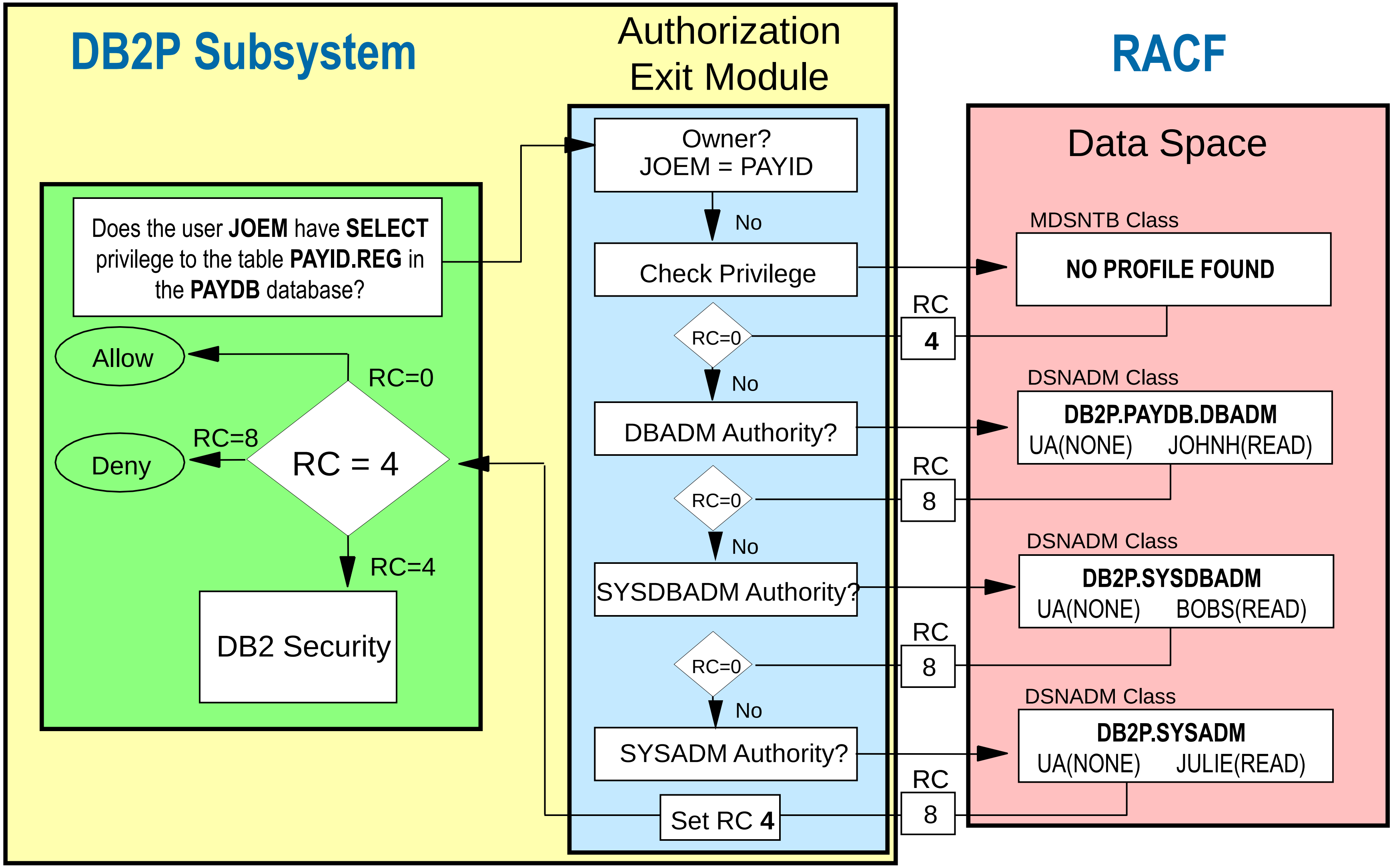
Access Allowed By Admin Authority



Access Allowed By Admin Authority



Access for Unprotected Objects



DB2P Subsystem

Does the user **JOEM** have **SELECT** privilege to the table **PAYID.REG** in the **PAYDB** database?

Allow

Deny

RC=0

RC=8

RC = 4

RC=4

DB2 Security

Authorization Exit Module

Owner?
JOEM = PAYID

No

Check Privilege

RC=0

No

DBADM Authority?

RC=0

No

SYSDBADM Authority?

RC=0

No

SYSADM Authority?

Set RC **4**

RC **4**

RC 8

RC 8

RC 8

RACF

Data Space

MDSNTB Class

NO PROFILE FOUND

DSNADM Class

DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

DSNADM Class

DB2P.SYSDBADM
UA(NONE) BOBS(READ)

DSNADM Class

DB2P.SYSADM
UA(NONE) JULIE(READ)

DB2 Access Events Logged to SMF

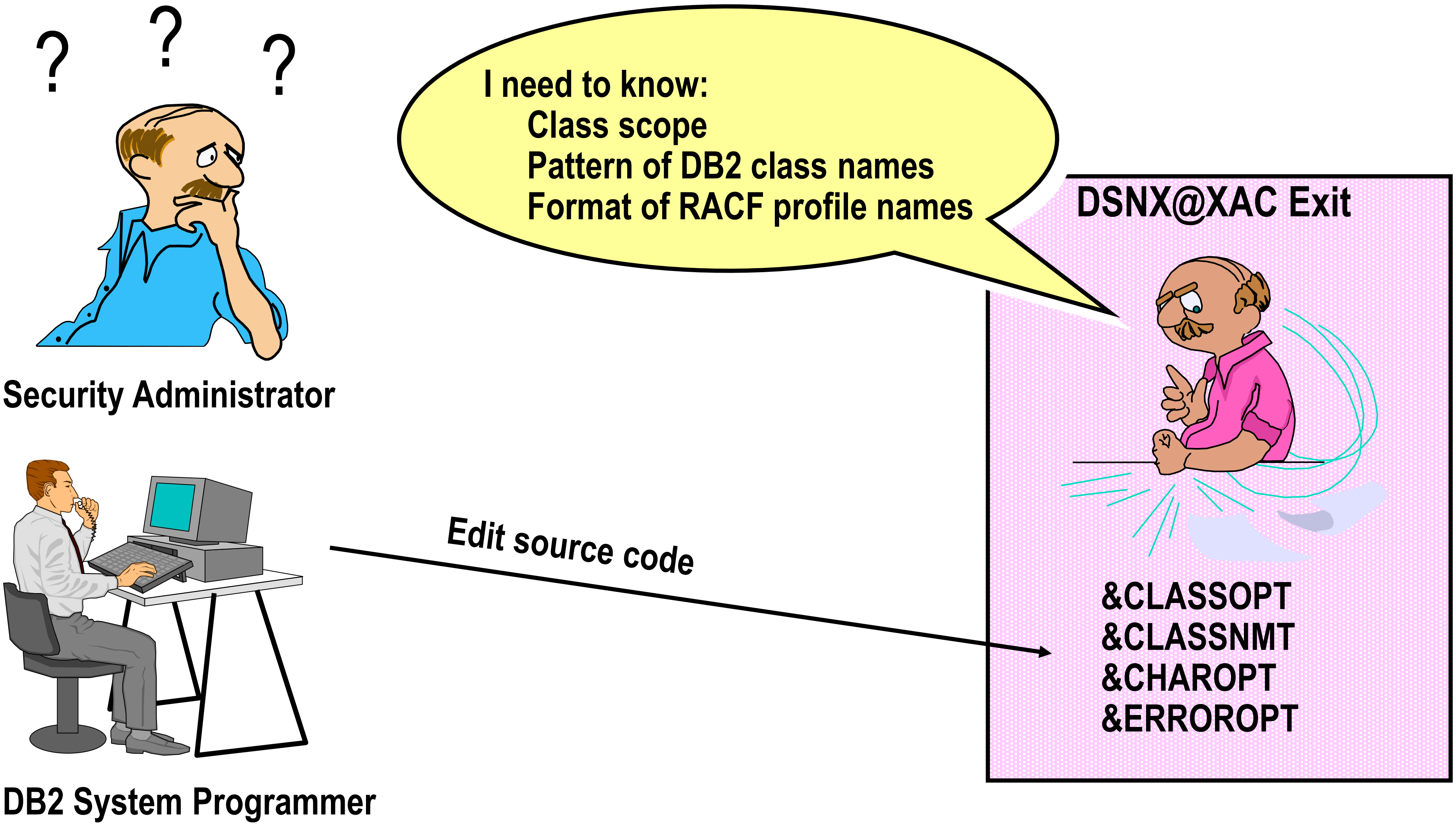
Violations

- After RACF has checked all object profiles
- After RACF has checked all authority profiles
- The final resulting return code is 8
- AUDIT(FAILURES) in object profile

Successes

- A RACF profile has allowed access (RC=0)
- AUDIT(SUCCESS) in profile

Customizing the DSNX@XAC Exit



I need to know:
- Class scope
- Pattern of DB2 class names
- Format of RACF profile names

Security Administrator

DSNX@XAC Exit

Edit source code

&CLASSOPT
&CLASSNMT
&CHAROPT
&ERROROPT

DB2 System Programmer

Customization Options for DSNX@XAC

&CLASSOPT Class Scope

1 = Single-subsystem scope
2 = Multi-subsystem scope

&CLASSNMT Class Name Root

Only applicable for &CLASSOPT=2
Default is ‘DSN’ to use predefined classes
1 to 4 characters

&CHAROPT Class Name Suffix

Last character of classname: 0 - 9, #, @, $
Default is ‘1’

&ERROROPT

1 = Defer to DB2 when an unexpected error occurs
2 = Instruct DB2 to terminate when an unexpected error occurs

↑

Unexpected errors: DSNX@XAC Abends, unexpected return codes

Multi-Subsystem Scope Options

Example of using the default settings:

Exit options

&CLASSOPT = 2
&CLASSNMT = DSN
&CHAROPT = ‘ ‘

Classes for DB2 Objects

MDSNTB
GDSNTB
MDSNPN
GDSNPN
Etc.

Class for DB2 Authorities

DSNADM

Profile names *must* be prefixed with DB2 subsystem name

Single-Subsystem Scope Options

Example of installation-defined classes

Exit options

&CLASSOPT = 1
&CLASSNMT = Not Applicable (DB2 subsys name is used)
&CHAROPT = #

Classes for DB2 Objects

MDB2PTB#
GDB2PTB#
MDB2PPN#
GDB2PPN#
Etc.

MDB2TTB#
GDB2TTB#
MDB2TPN#
GDB2TPN#
Etc.

Class for DB2 Authorities

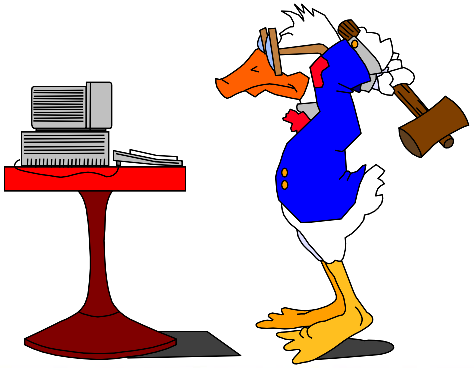
DB2PADM#

DB2TADM#

Profile names are *not* prefixed with DB2 subsystem name

Steps To Implement DSNX@XAC Exit

1. Obtain sample RACF Access Control Module
   - From *prefix*. SDSNSAMP(DSNXRXAC)
2. Copy to a private library with name of DSNX@XAC
3. Specify the exit options (optional)
   - &CLASSOPT
   - &CLASSNMT
   - &CHAROPT
   - &ERROROPT
4. Define & activate DB2 classes in CDT class (optional)
5. Assemble and link edit the sample exit
6. Run DSNTIJEX install job
   - Replaces dummy DNSX@XAC
7. Start DB2



Running the RACFDB2 Utility

- Download the RACF to DB2 utility via WWW or FTP
- User running the tool must have SELECT privilege on the SYSIBM.SYSxxxAUTH tables
- Specify values for
  - Owner for profiles
  - DB2 subsystem name
  - Class name root
  - Single subsystem or multi-subsystem
  - Last character of class name

RACFDB2 Generated Commands

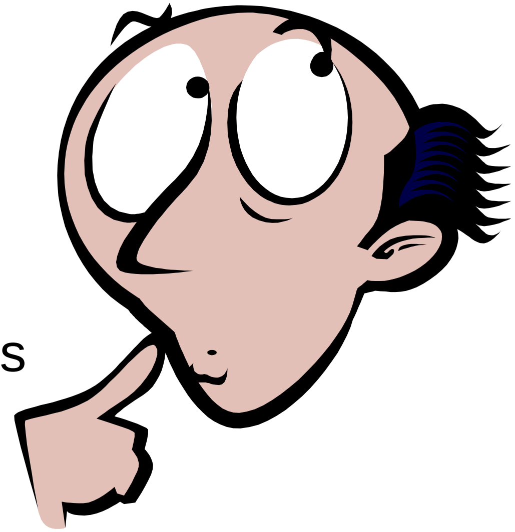
- Discrete profile RDEFINE commands for all objects, privileges and authorities
- UACC is set to READ for objects granted to PUBLIC
- AUDIT(ALL(READ)) is set for DB2 administrative authorities
- PERMIT DELETE command generated for each profile
- PERMIT with ACCESS(ALTER) if authorized ‘WITH GRANT’ option
- PERMIT with ACCESS(READ) if authorized without GRANT option
- PERMIT commands are generated for all GRANT statements, including users with SYSADM
- PERMIT commands are generated for all GRANT statements on tables for the table owner
- All RDEFINE commands are for profiles in the member classes

RACFDB2 Generated Commands

- Edit the generated commands
  - Remove or modify unnecessary commands
- Consider replacing many of the discrete profiles!
  - Use generic profiles?
  - Use some grouping profiles?
  - Use RACFVARS variables for privilege qualifiers?
- Define RACF classes for DB2 if using Single-Subsystem Scope
- Enable Generic profiles for the RACF classes to be used for DB2
- Activate the DB2 general resource classes
- Execute the generated RACF commands

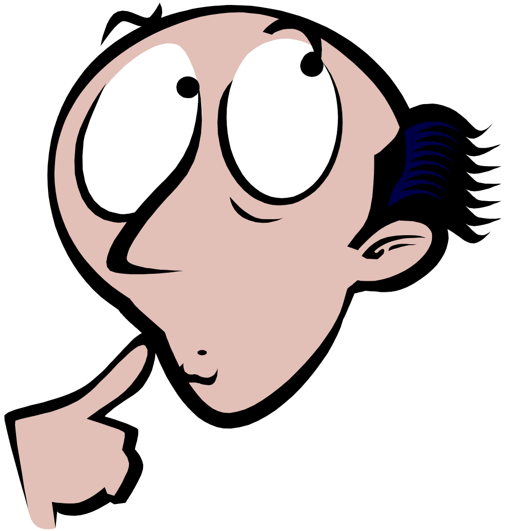
Migration Considerations

- Differences between (internal) DB2 and RACF security
  (See DB2 for z/OS RACF Access Control Module Guide, Chapter 10. Special Considerations)
  - Materialized query tables
  - PUBLIC* (DB2 V9)
  - Authorization for implicitly created databases
  - Authorization checking for operations on views
  - Implicit privileges of ownership
  - Matching schema names
  - ALTER and DROP Index
  - CREATETMTAB, CREATE VIEW, & CREATE ALIAS privileges
  - “Any table” and “any schema” privileges
  - GRANT statements
  - . . .



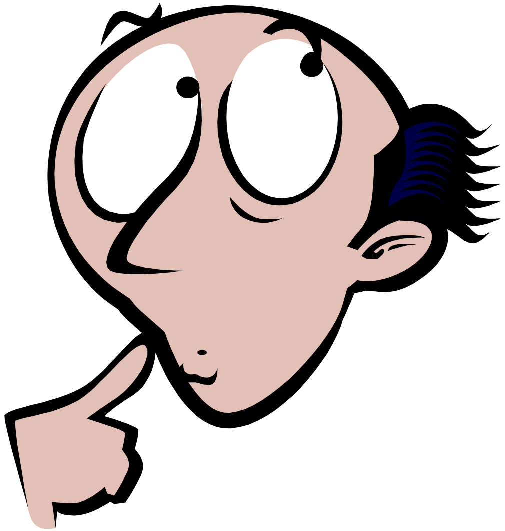
Migration Considerations

- Software, applications, tools that use the security tables in DB2 catalog?



Migration GOTCHAs

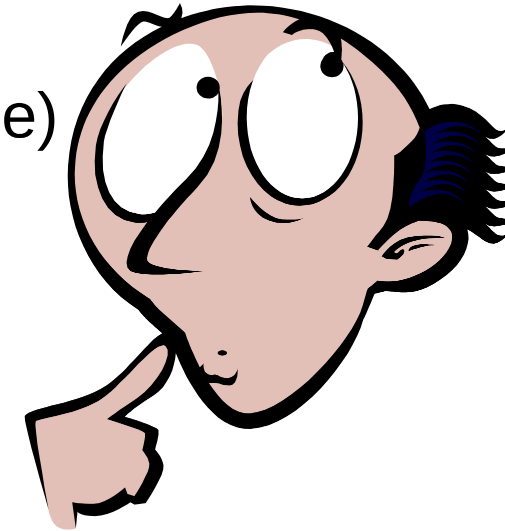
- The IBM tool only converts 9 of the object types.
- It does not convert:
  - Sequences
  - JARS
  - Stored Procedures
  - User Defined Distinct Types
  - User Defined Functions
  - Schemas



Note: Vanguard's DB2 Migration Tool creates the required profiles for these additional object types.

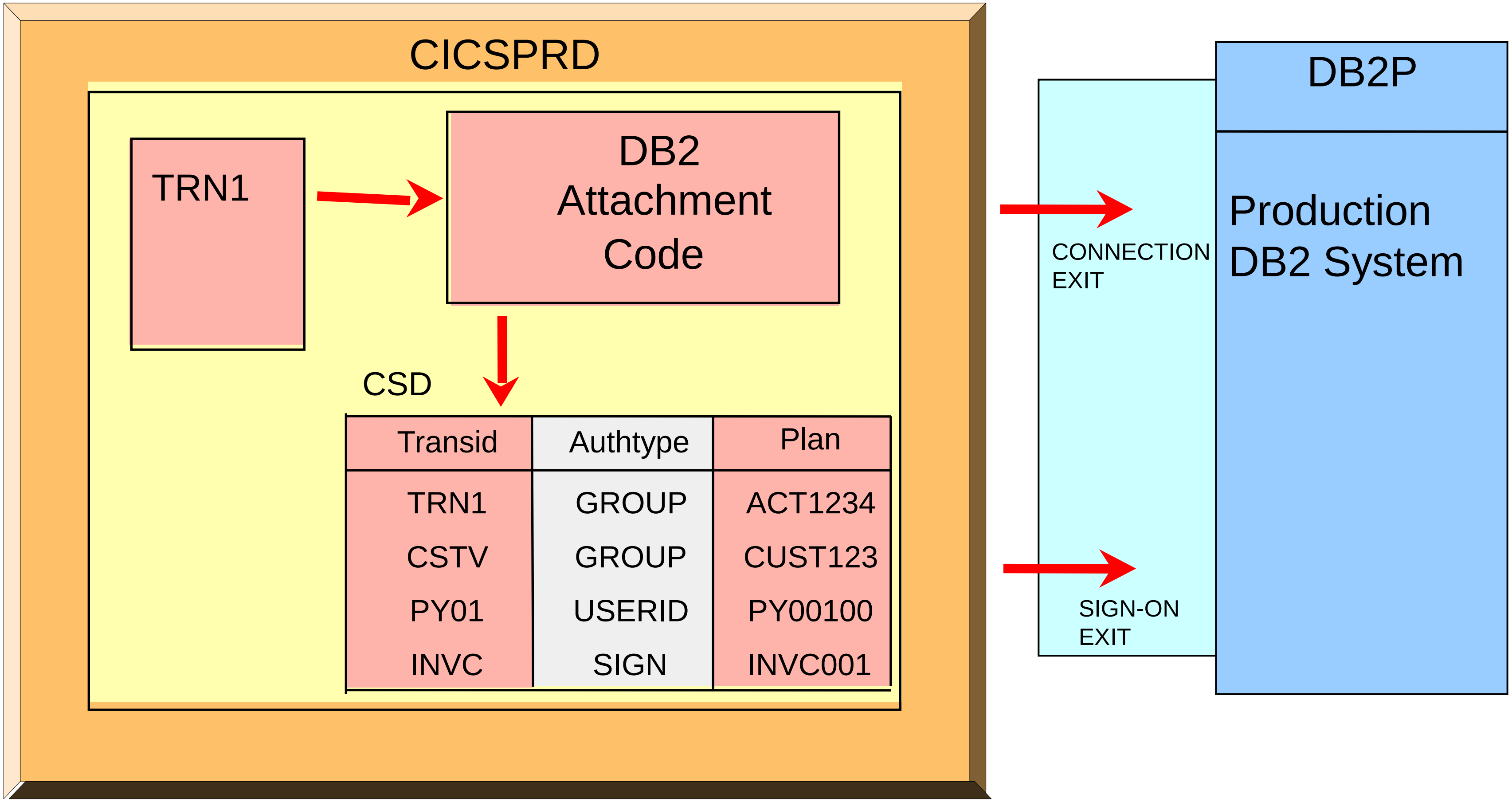
Migration GOTCHAs

- The IBM tool does not handle the new format for View authorities for INSERT, UPDATE and DELETE.
- DYNAMIC tables and Views.
- Create ** profile in all DB2 classes with UACC(NONE) and no access list.
- CICS® Connection Entries (next slide)



Note: Vanguard's DB2 Migration Tool correctly creates the new VIEW profile formats.

Migration GOTCHAs



Transid	Authtype	Plan
TRN1	GROUP	ACT1234
CSTV	GROUP	CUST123
PY01	USERID	PY00100
INVC	SIGN	INVC001

Note: AUTHTYPE(SIGN), when SIGNID(CICS_region_user id) passes CICS region ACEE
AUTHID(string) does not pass an ACEE To the Security Exit.

Key Migration Benefits

Centralized Mainframe Security Management for DB2 in RACF

Seperation of Duties

Migration to RACF ensures security is managed by RACF administrators versus Database Administrators to ensure separation of duty.

1

Risk Reduction

Migration to RACF reduces operational risk as security is managed within RACF and reduces cost as no additional tools are needed to manage security within DB2.

2

Compliance

Migration to RACF streamlines and improves your audit and compliance processes as you will be able to leverage your Vanguard tools investment .

3

Security

Migration to RACF improves your overall security posture as you now have visbility through your existing Vanguard tools into the security of DB2.

4

DB2 Release Considerations

- On August 3, 2010, IBM announced the End of Service (EOS) for DB2 8 for z/OS. The effective EOS date is April 30, 2012.
- On February 7, 2012, IBM announced the End of Service (EOS) for DB2 9 for z/OS. The effective EOS date is June 27, 2014.
- On October 19, 2010, IBM announced General Availability for DB2 10 for z/OS as of October 22, 2010.
- On October 3, 2012, IBM announced an Early Support Program for DB2 11 for z/OS.

Planned Enhancements beyond DB2 V10

- Further External Security (DSNX@XAC) consistency with DB2 (internal) security
  - Allow owner to be checked on BIND and REBIND
  - Support Dynamic SQL authorization using DYNAMICRULES behavior
  - Allow automatic REBIND
- Refresh authorization related caches and invalidate dependent packages when external security permissions change

Bibliography for DB2 Version 9

- DB2 V9R1 for z/OS RACF Access Control Module Guide, SC18-9852-06
- DB2 V9R1 for z/OS Managing Security, SC19-3495-03

- DB2 V9R1 for z/OS Administration Guide, SC18-9840-15
- DB2 V9R1 for z/OS SQL Reference, SC18-9854-15
- DB2 V9R1 for z/OS Command Reference, SC18-9844-09
- DB2 V9R1 for z/OS Utility Guide and Reference, SC18-9855-14

Bibliography for DB2 Version 10

- DB2 V10R1 for z/OS RACF Access Control Module Guide, SC19-2982-06
- DB2 V10R1 for z/OS Managing Security, SC19-3496-03
- Security Functions of IBM DB2 V10 for z/OS, SG24-7959-00

- DB2 V10R1 for z/OS Administration Guide, SC19-2968-08
- DB2 V10R1 for z/OS SQL Reference, SC19-2983-09
- DB2 V10R1 for z/OS Command Reference, SC19-2972-05
- DB2 V10R1 for z/OS Utility Guide and Reference, SC19-2984-08

Thank You!

For more information, please visit:
http://www.go2vanguard.com or
e-mail: sales@go2vanguard.com

Thank You
English

ขอบคุณ
Thai

شكرا
Arabic

Gracias
Spanish

Danke
German

Obrigado
Brazilian Portuguese

Grazie
Italian

多谢
Simplified Chinese

Спасибо
Russian

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean

धन्यवाद
Hindi

多謝
Traditional Chinese

Merci
French