RACF for DB2 Control – Beyond the Basics

Doug Behrends

Vanguard Professional Services

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Legal Notice

Copyright

Trademarks

The following are trademarks of Vanguard Integrity Professionals – Nevada:

- Vanguard Administrator
- Vanguard Advisor
- Vanguard Analyzer
- Vanguard SecurityCenter
- Vanguard Offline
- Vanguard Cleanup
- Vanguard PasswordReset
- Vanguard Authenticator
- Vanguard inCompliance
- Vanguard IAM
- Vanguard GRC
- Vanguard QuickGen
- Vanguard Active Alerts
- Vanguard Compliance Manager
- Vanguard Configuration Manager
- Vanguard Policy Manager
- Vanguard Enforcer
- Vanguard Alert Connector
- Vanguard ez/Token
- Vanguard Tokenless Authenticator
- Vanguard ez/PIV Card Authenticator
- Vanguard ez/Integrator
- Vanguard ez/SignOn
- Vanguard ez/Password Synchronization
- Vanguard Security Solutions
- Vanguard Security & Compliance
- Vanguard zSecurity University

Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation:

CICS	IMS	S/390	z9
CICSPlex	MQSeries	System z	z10
DB2	MVS	System z9	z13
eServer	NetView	System z10	z14
IBM	OS/390	System/390	z/Architecture
IBM z	Parallel Sysplex	VTAM	z/OS
IBM z Systems	RACF	WebSphere	z/VM
IBM z14	RMF	z Systems	zEnterprise

Java and all Java-based trademarks are trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

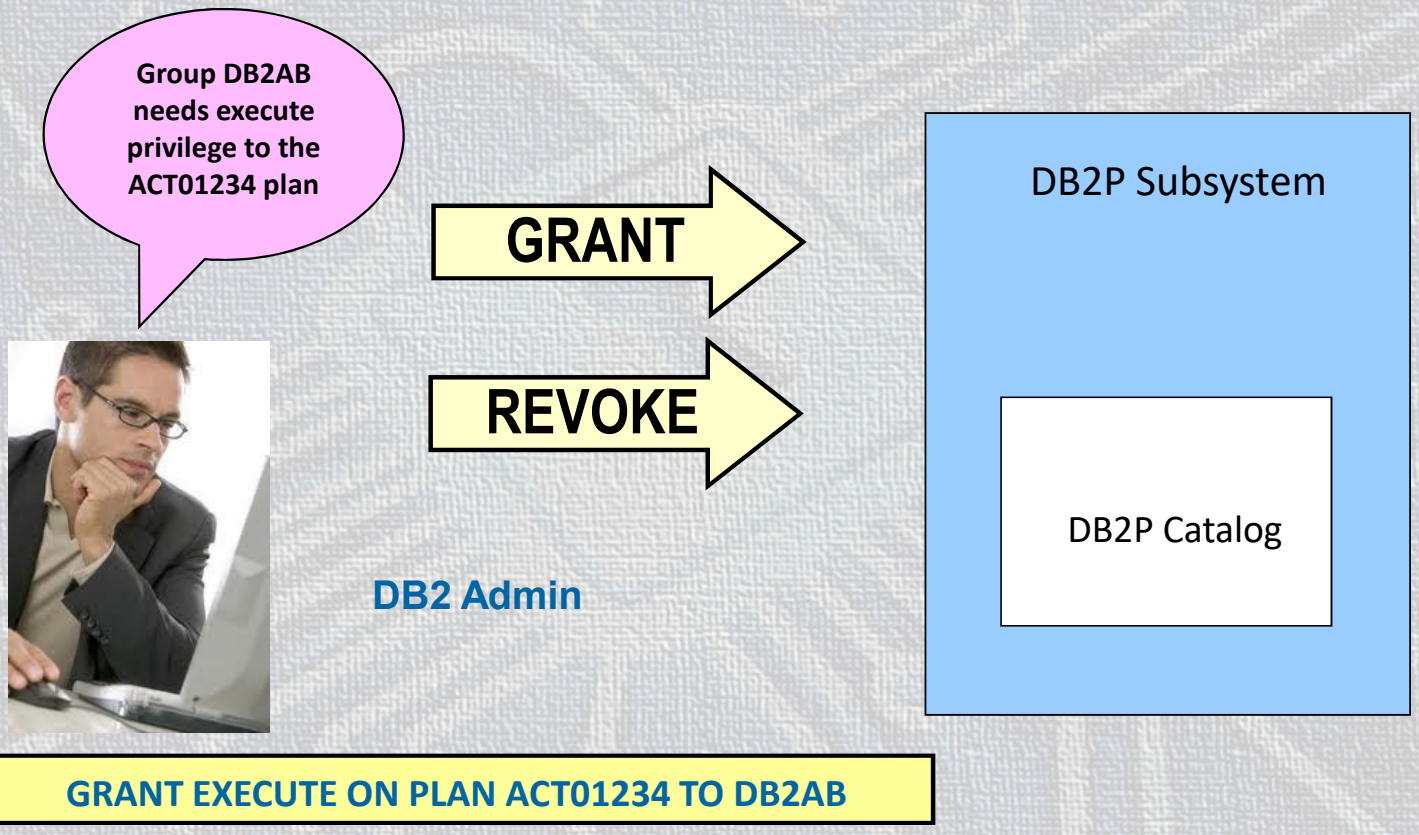
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

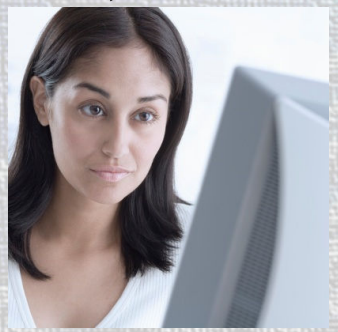
Session Topics

RACF Security for DB2 Objects

Traditional DB2 Security



RACF Security for DB2 Objects



RACF Admin

Group DB2AB needs execute privilege to the ACT01234 plan in the DB2P subsystem

RDEFINE

RALTER

PERMIT

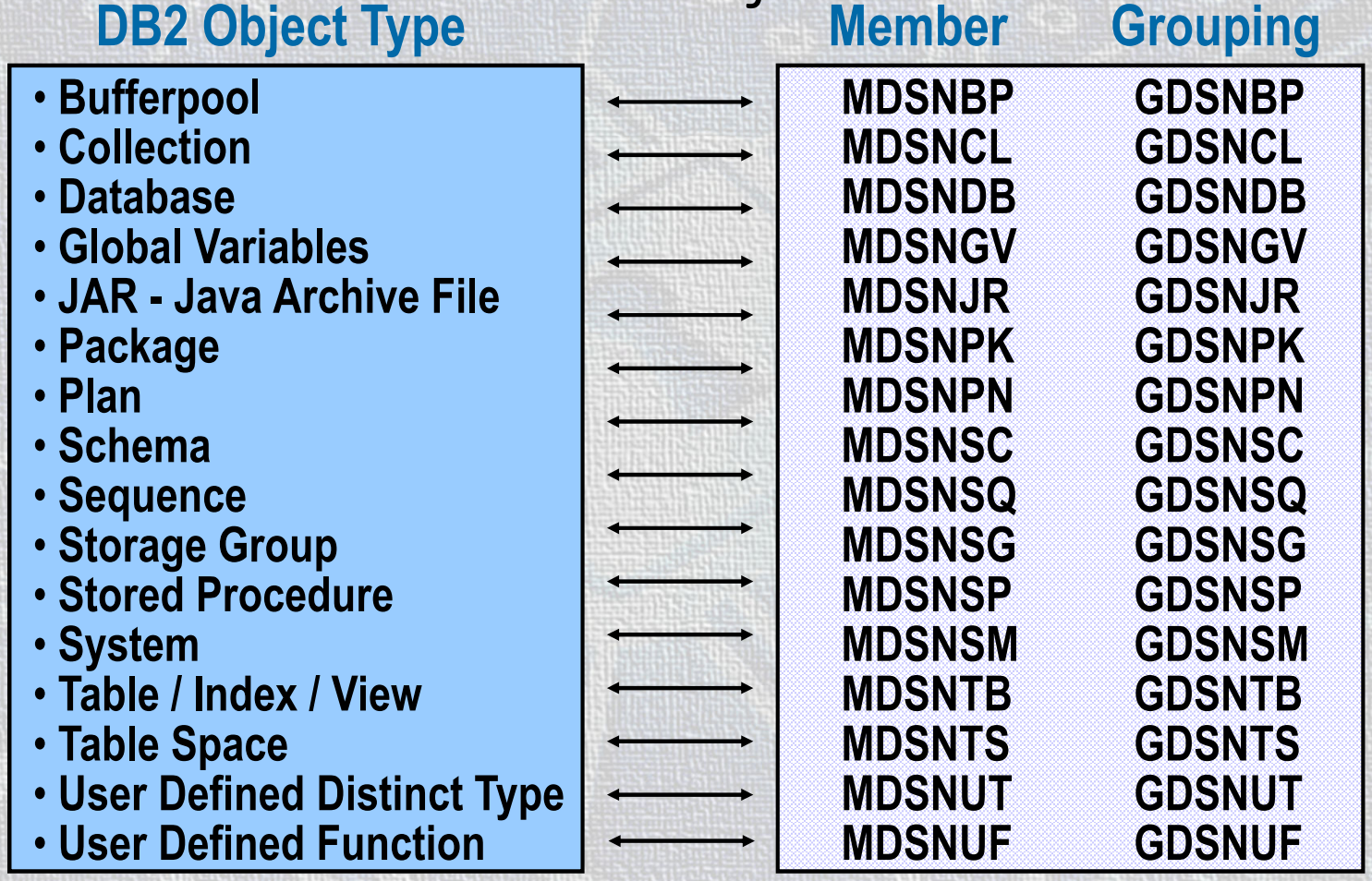
RACF

RACF Database

RDEF MDSNPN DB2P.ACT01234.EXECUTE OW(DB2ADM) UA(NONE)

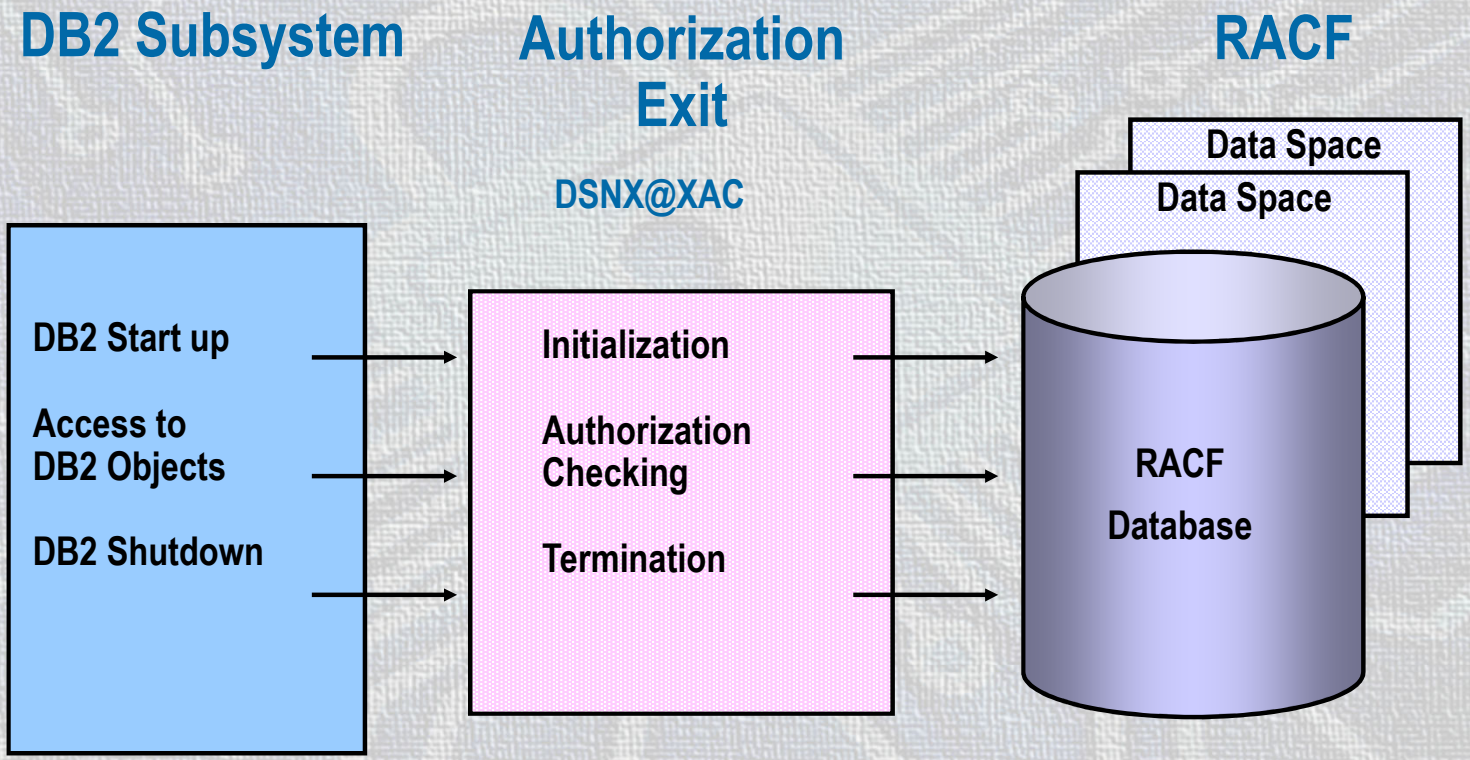
PE DB2P.ACT01234.EXECUTE CLASS(MDSNPN) ID(DB2AB) AC(READ)

RACF Classes For DB2 Objects



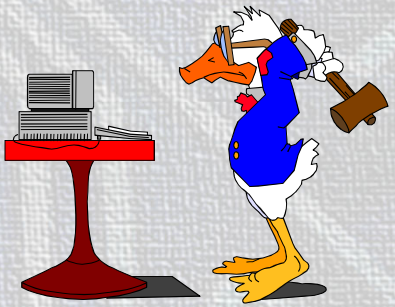
RACF Access Control Module

DB2 Authorization Exit



Steps To Implement DSNX@XAC Exit

1. **Obtain the RACF Access Control Module**
   - From *prefix*.SDSNSAMP(DSNXRXAC) – starting with DB2 V8
2. **Copy to a private library with name of DSNX@XAC**
3. **Specify the exit options (optional)**
   - &CLASSOPT
   - &CLASSNMT
   - &CHAROPT
   - &ERROROPT
4. **Define DB2 classes in CDT (if exit modified)**
5. **Define RACF profiles - RDEFINE, RALTER, PERMIT**
6. **Activate the DB2 classes**
7. **Assemble and link edit the sample exit**
   - Modify JEX0003 step of DB2 install job
   - Run JEX0003 job
8. **Start DB2**



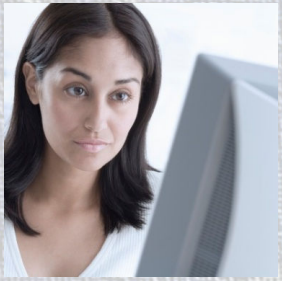
Single or Multi-Subsystem Scope?

- Multi-Subsystem Scope Classes
  - Default
  - First qualifier is DB2 subsystem name
  - No changes to CDT

- Single Subsystem Scope Classes
  - Optional
  - DB2 subsystem name not in profile
  - Add classes to CDT

Customizing the DSNX@XAC Exit

? ? ?



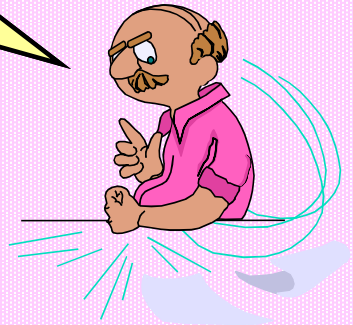
Security Administrator

System Programmer

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

Edit source code

DSNX@XAC Exit



&CLASSOPT
&CLASSNMT
&CHAROPT
&ERROROPT

Customization Options for DSNX@XAC

&CLASSOPT Class Scope

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

&CLASSNMT Class Name Root

1 to 4 characters
'DSN' is the default
Only for &CLASSOPT=2
Example: MDB2PTB

&CHAROPT Class Name Suffix

Last character of classname
0 - 9, #, @, $
Default is '1'
Example: MDB2PTB#

Customization Options for DSNX@XAC

&ERROROPT

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

An unexpected error is:

- **DSNX@XAC abends**
- **DSNX@XAC returns an unexpected return code**
- **DSNX@XAC instructs DB2 to not call it again**

Multi-Subsystem Scope Options

Example of using the default settings:

Exit options

&CLASSOPT = 2
&CLASSNMT = DSN

Classes for DB2 Objects

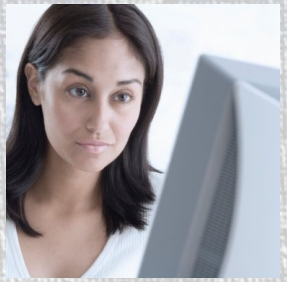
MDSNTB
GDSNTB
MDSNPN
GDSNPN
Etc.

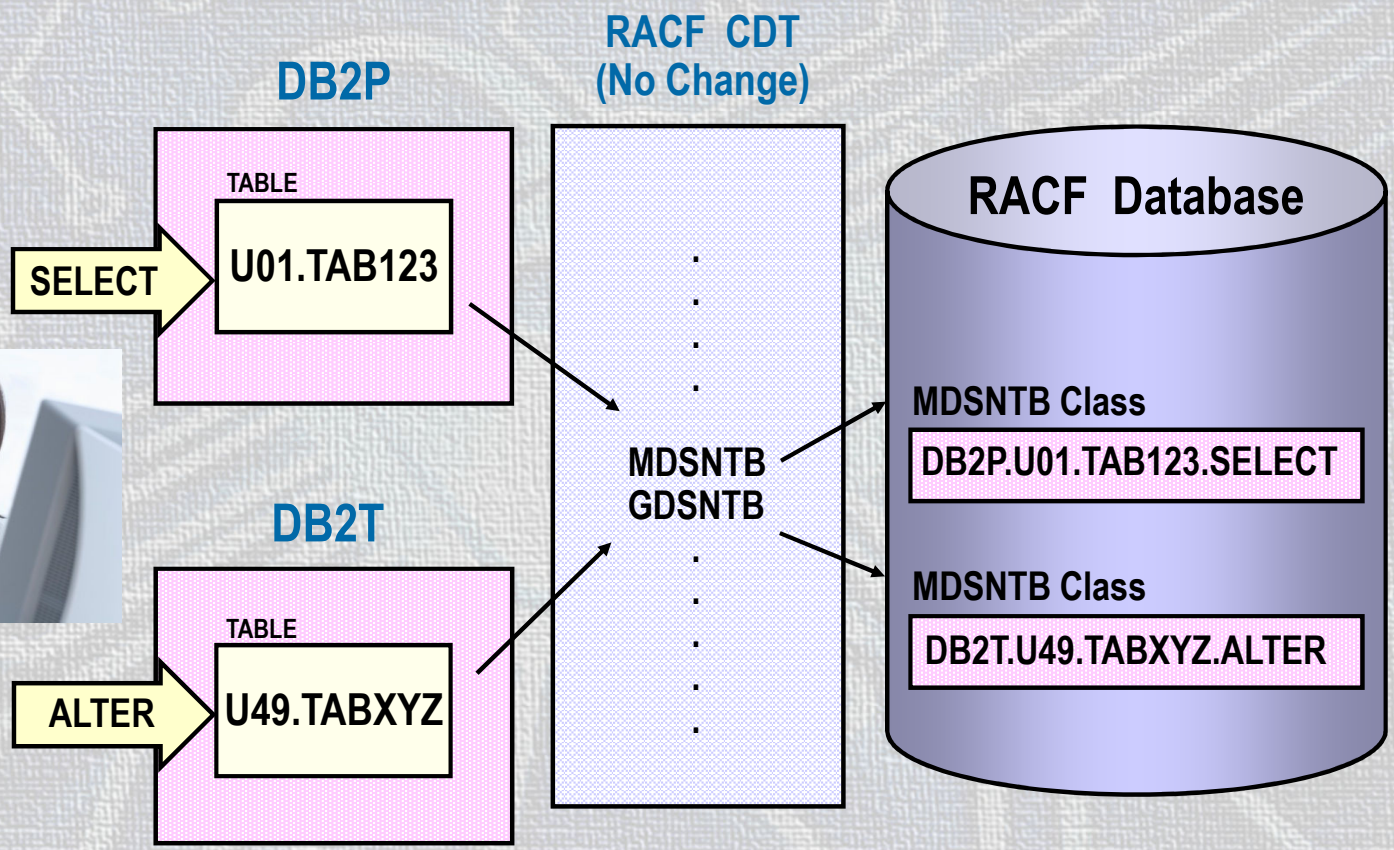
Class for DB2 Authorities

DSNADM

Profile names *must* be prefixed with DB2 subsystem name

Multi-Subsystem Scope (Default)





Single-Subsystem Scope Options

Example of installation-defined classes

Exit options

&CLASSOPT = 1
&CLASSNMT = Not Applicable
&CHAROPT = #

Classes for DB2 Objects

MDB2PTB#	MDB2TTB#
GDB2PTB#	GDB2TTB#
MDB2PPN#	MDB2TPN#
GDB2PPN#	GDB2TPN#
Etc.	Etc.

Class for DB2 Authorities

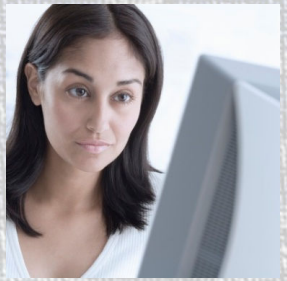
DB2PADM# DB2TADM#

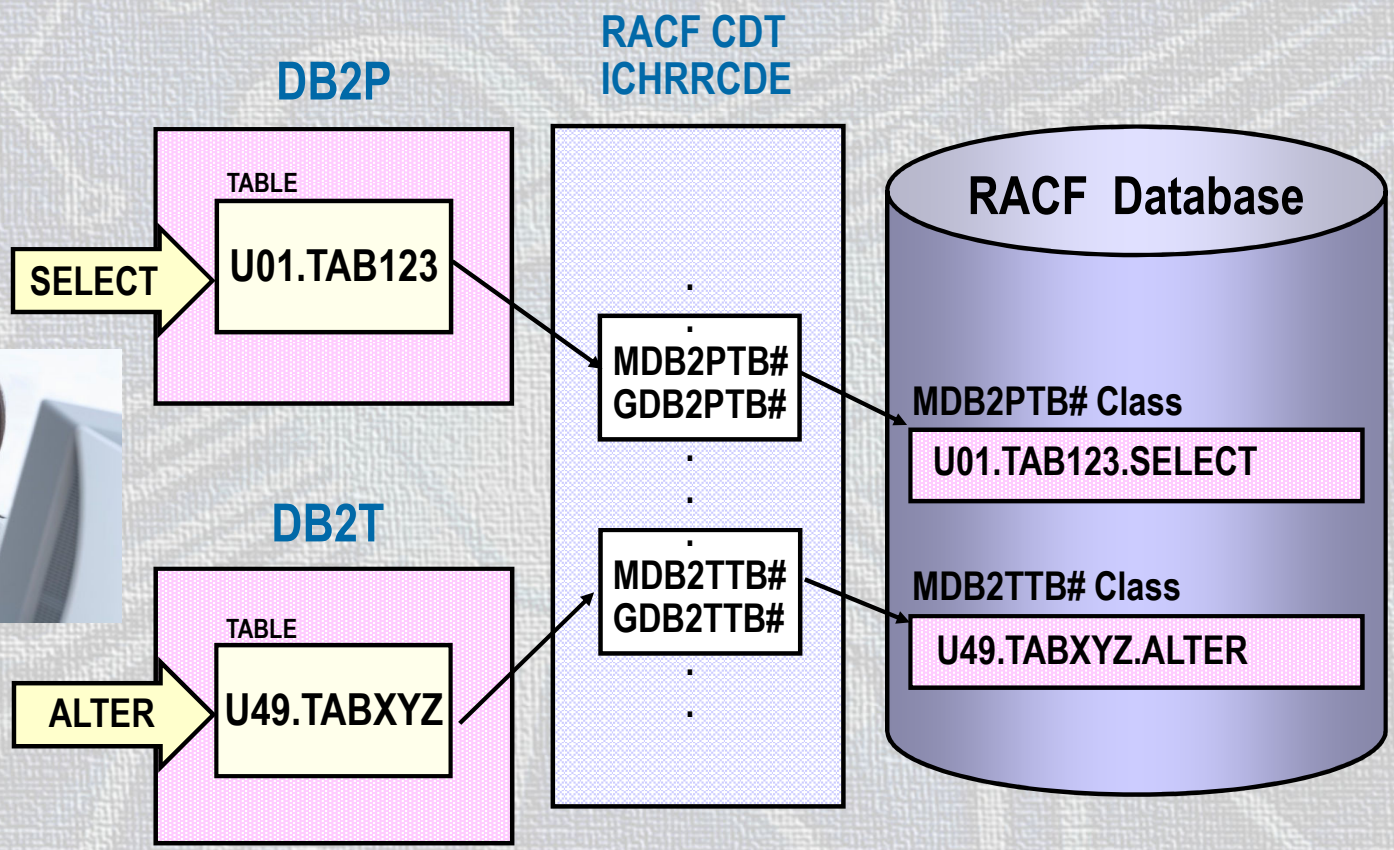
Profile names are *not* prefixed with DB2 subsystem name
Class names *must* contain DB2 subsystem name

Dynamic CDT

```
RDEFINE  CDT  MDB2PTB#
                CDTINFO(DEFAULTUACC(NONE)
                FIRST(ANY)  OTHER(ANY)
                MAXLNTH(100)
                GROUP(GDB2PTB#)
                OPER(N0)
                DEFAULTRC(4)
                POSIT(526)
                SIGNAL(YES)
                RACLIST(REQUIRED))
RDEFINE  CDT  GDB2PTB#
                CDTINFO(DEFAULTUACC(NONE)
                FIRST(ANY)  OTHER(ANY)
                MAXLNTH(100)
                MEMBER(MDB2PTB#)
                OPER(N0)
                DEFAULTRC(4)
                POSIT(526)
                SIGNAL(YES)
                RACLIST(REQUIRED))
```

Single-Subsystem Scope

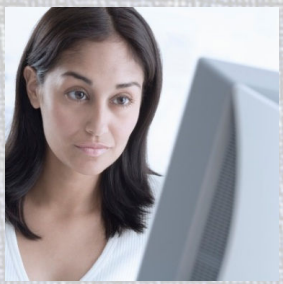


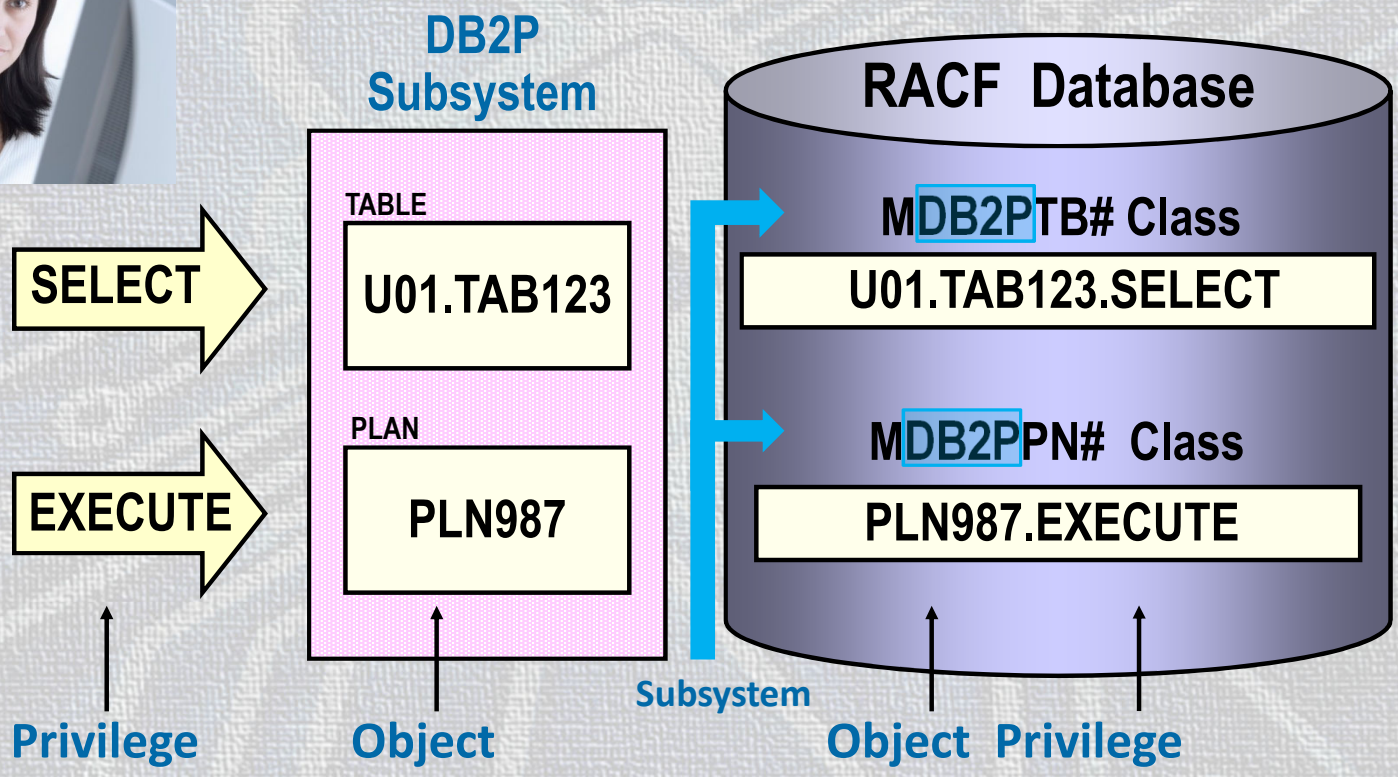


VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

RACF Profiles for DB2 Objects

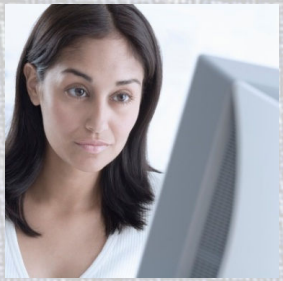
RACF Profile Syntax - Single-Subsystem Scope

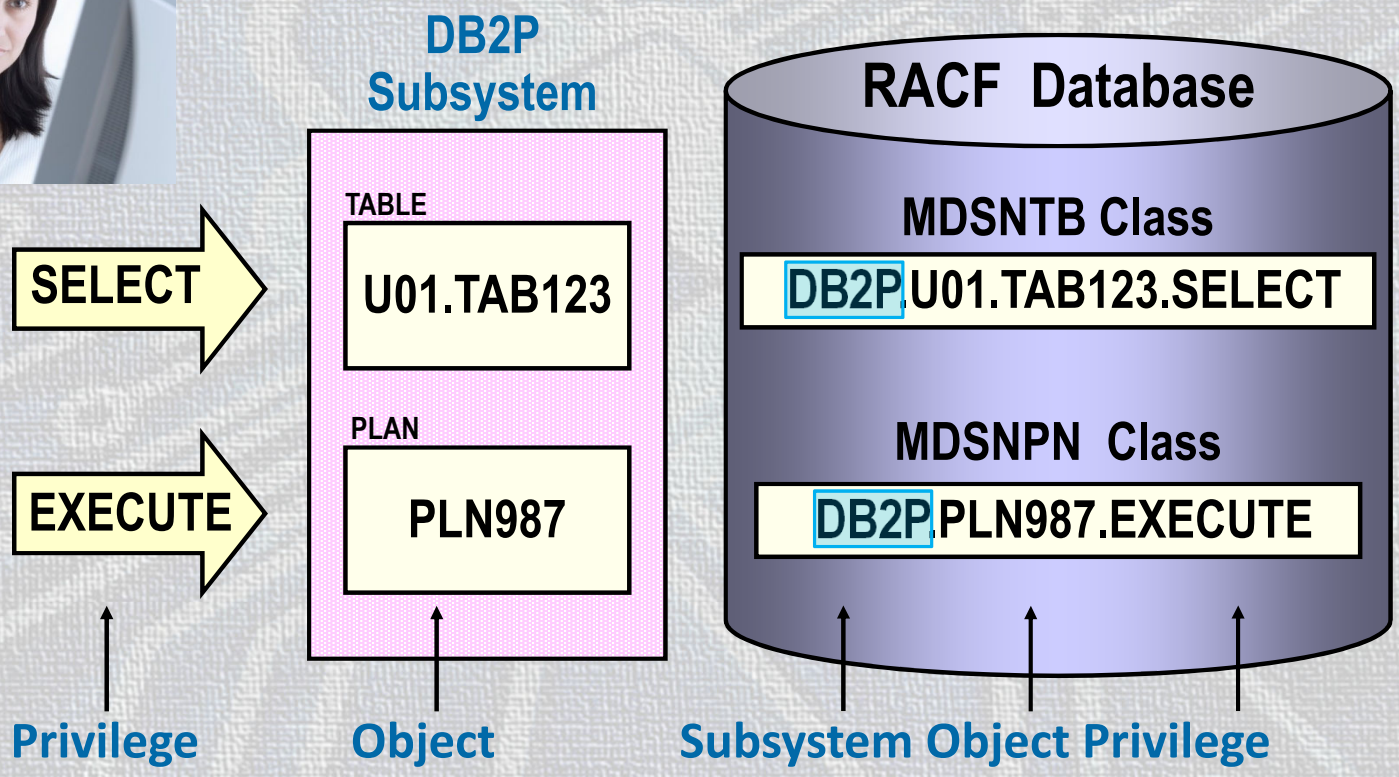




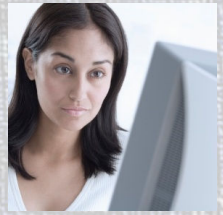
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

RACF Profile Syntax - Multi-Subsystem Scope





Profiles for Databases



DB2-subsystem.database-name.privilege

Privilege

CREATETAB
CREATETS
DISPLAYDB
DROP
IMAGCOPY
LOAD
RECOVERDB
REORG
REPAIR
STARTDB
STATS
STOPDB

DB2P Subsystem

PAYDB Database

RACF Database

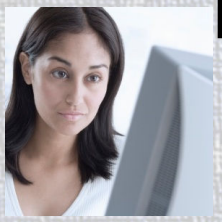
MDSNDB Class

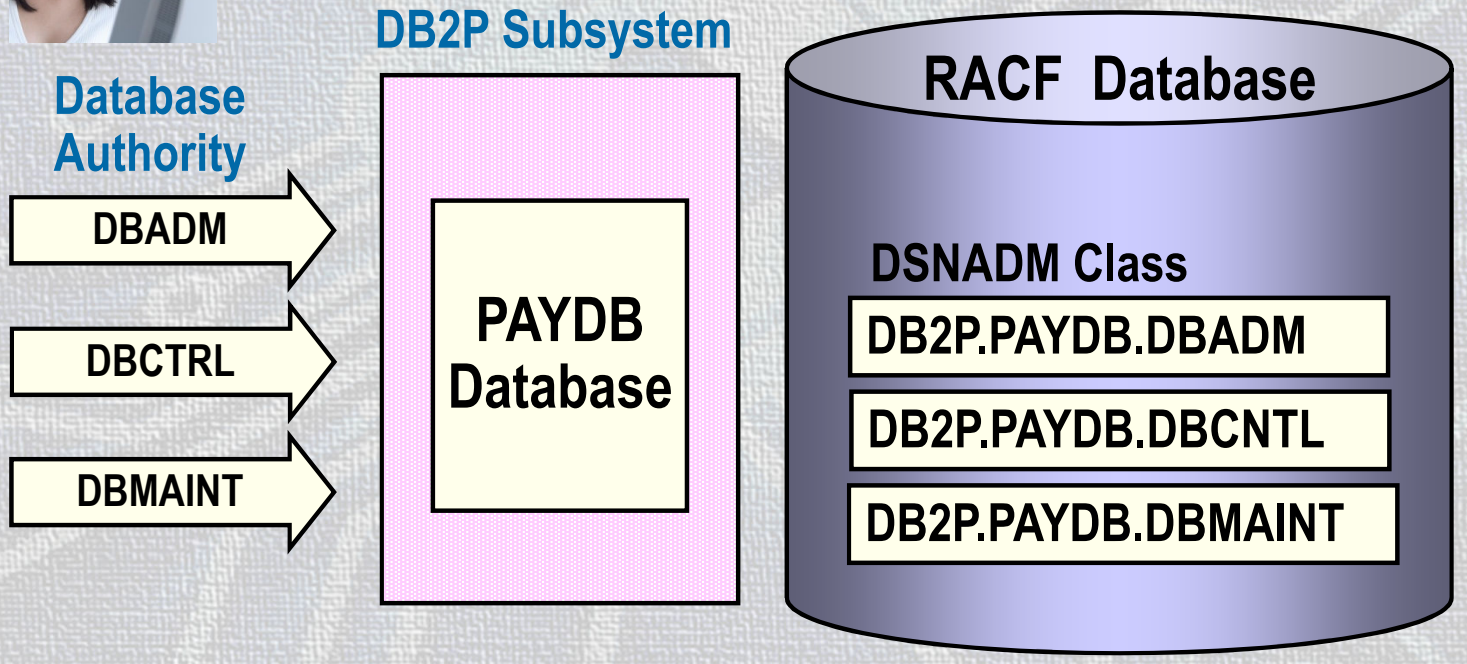
DB2P.PAYDB. *

DB2P.PAYDB.REORG

Profiles for Database Authority

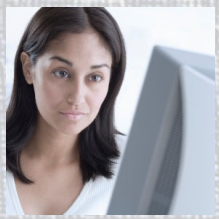
DB2-subsystem.Database-name.authority





Profiles for Tables

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



Valid privileges for table columns are
REFERENCES and UPDATE

Privilege

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

DB2P Subsystem

U01.TAB123

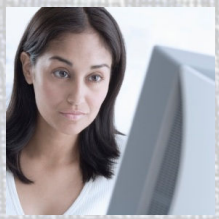
RACF Database

MDSNTB Class

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

Profiles for Views

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



Privilege

SELECT

DELETE
INSERT
UPDATE

DB2P Subsystem

U01.VIEW789

U01.TAB123

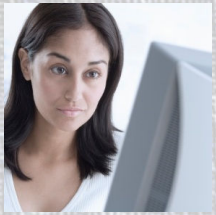
RACF Database

MDSNTB Class

DB2P.U01.VIEW789.SELECT

DB2P.U01.TAB123.U01.VIEW789.INSERT

Profiles for System Privileges



DB2-subsystem.privilege
DB2-subsystem.package-owner.BINDAGENT

Privilege

- ARCHIVE
- BINDADD
- BINDAGENT
- BSDS
- CREATEALIAS
- CREATEDBA
- CREATEDBC
- CREATESG
- CREATETMTAB
- DISPLAY
- EXPLAIN
- MONITOR1
- MONITOR2
- RECOVER
- STOPALL
- STOSPACE
- SQLADM
- TRACE

DB2P Subsystem

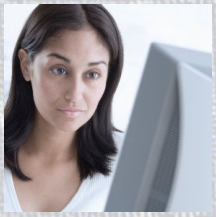
System Privileges

RACF Database

MDSNSM Class

- DB2P.CREATEDBA
- DB2P.SQLADM
- DB2P.*

Profiles for System Authorities



DB2-subsystem.authority

System Authority

ACCESSCTRL
DATAACCESS
SECADM
SYSADM
SYSCTRL
SYSDBADM
SYSOPR

DB2P Subsystem

System Authorities

RACF Database

DSNADM Class

DB2P.ACCESSCTRL

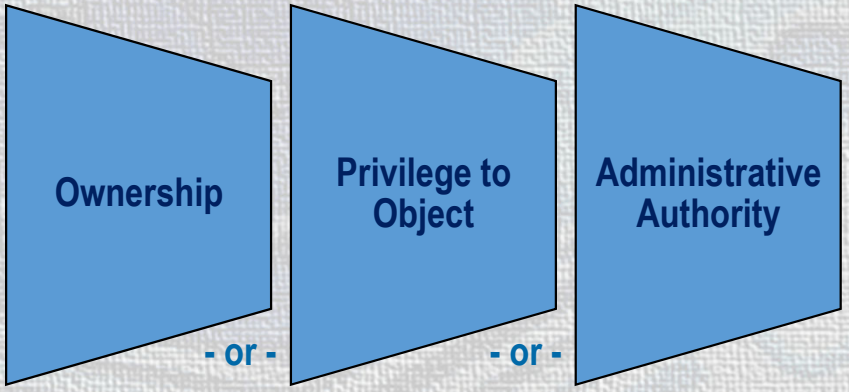
DB2P.SYSDBADM

DB2P.SYSADM

Controlling Access to DB2 Objects

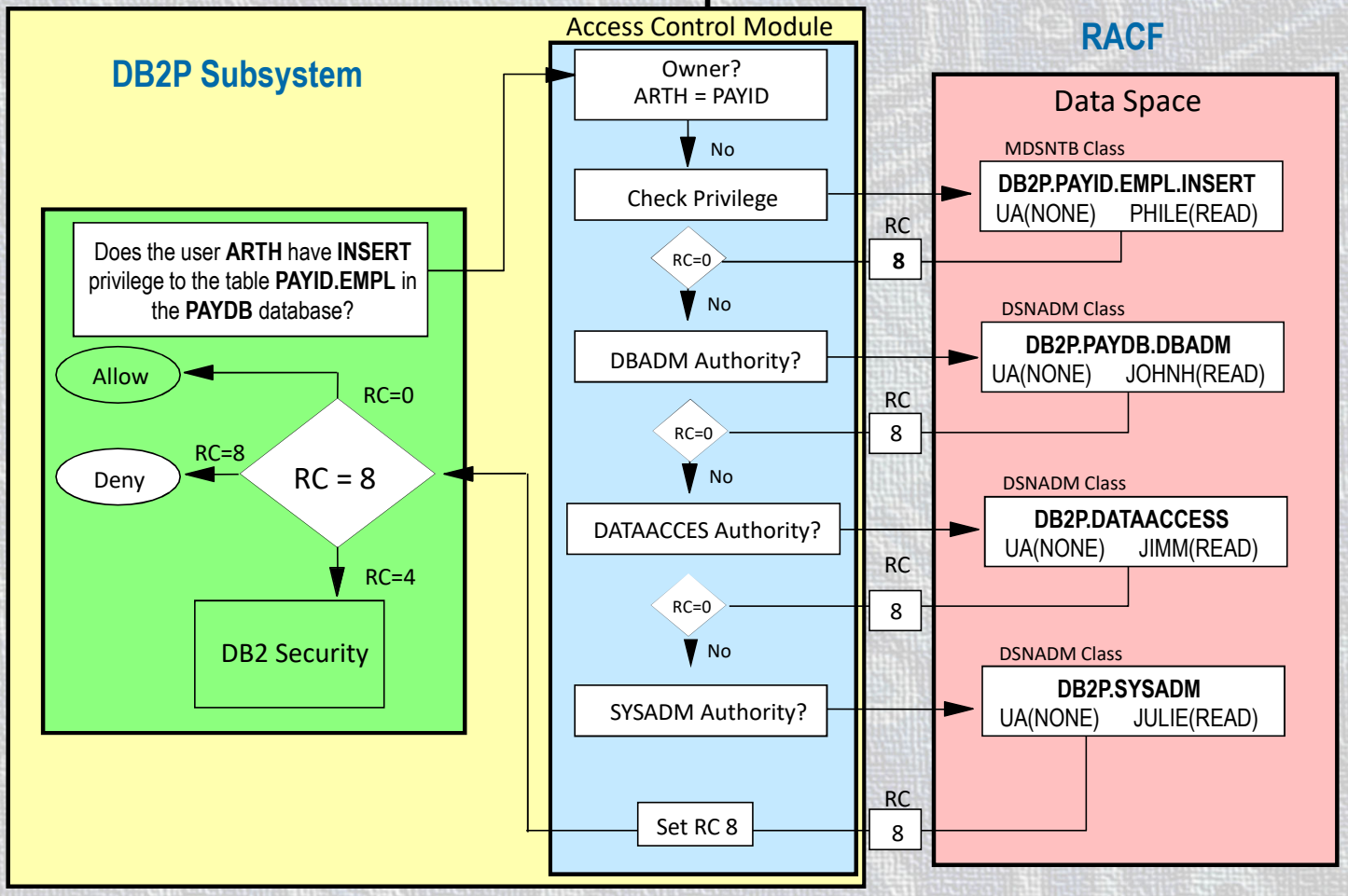
Access Control With RACF

- To access a DB2 object requires:



VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Authorization Exit Example

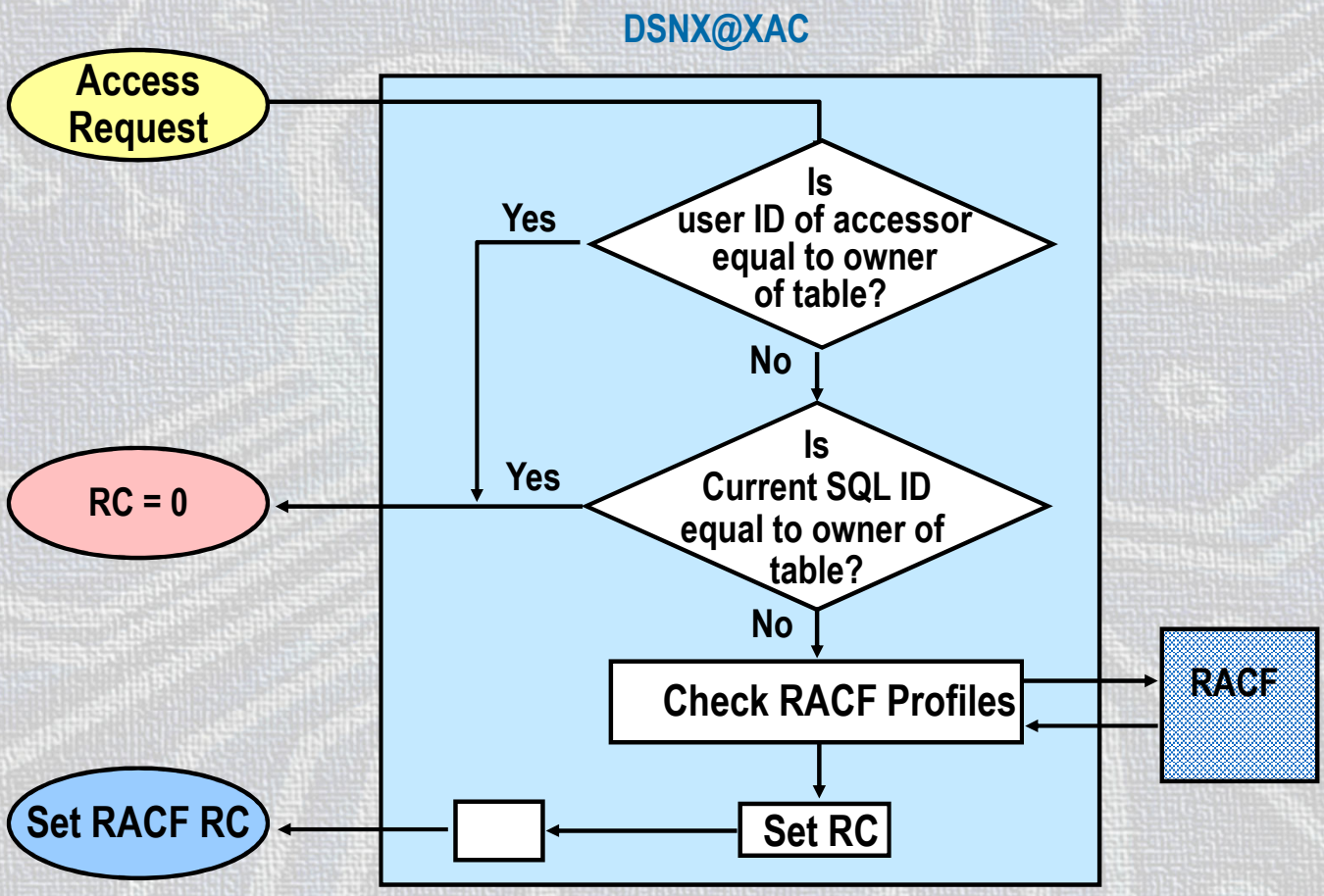


VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

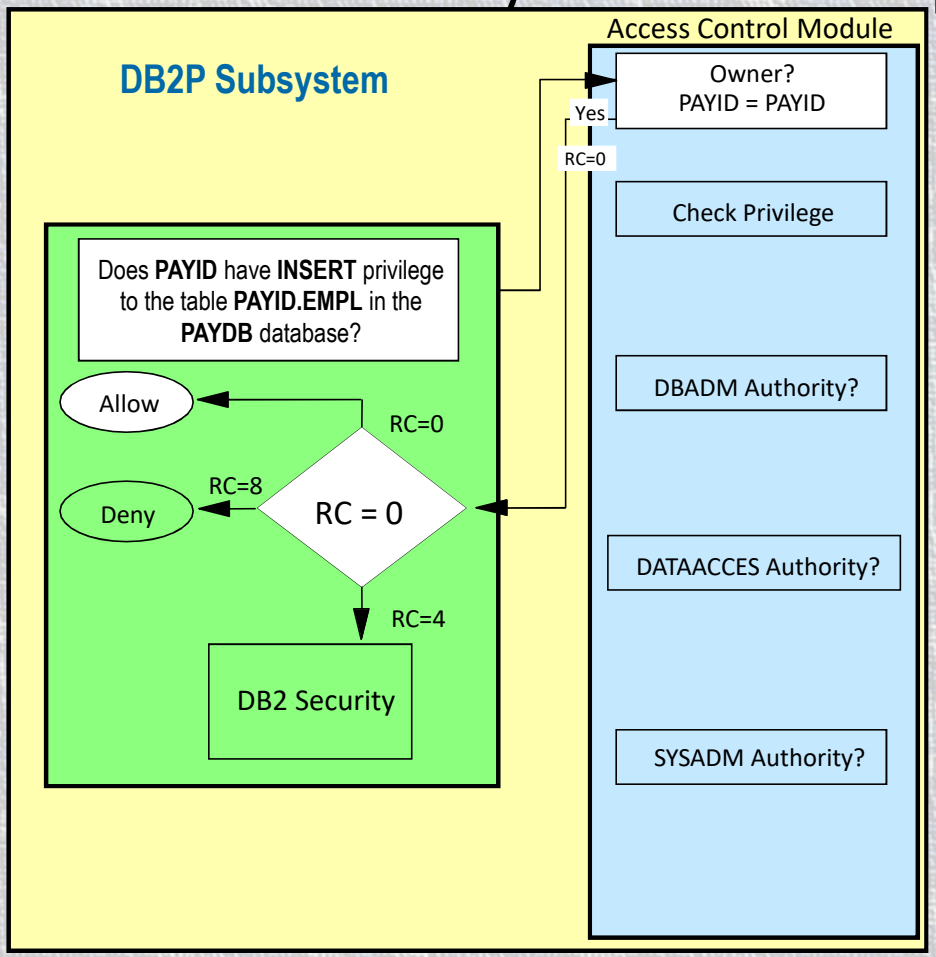
DSNX@XAC Exit Return Codes

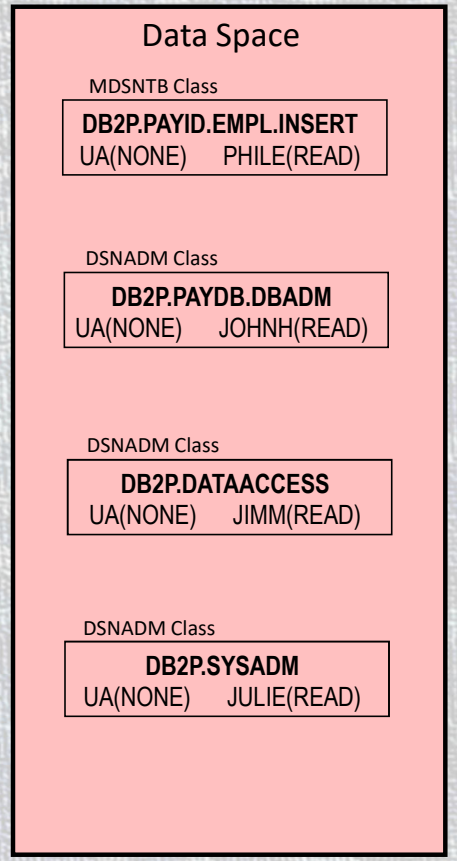
Return Codes from RACF		Return Code passed to DB2
Object Profile	DSNADM Profile	
0	Not Applicable	0
4	0	0
4	4	4
4	8	4
8	0	0
8	4	8
8	8	8

Implicit Privileges for Table Ownership



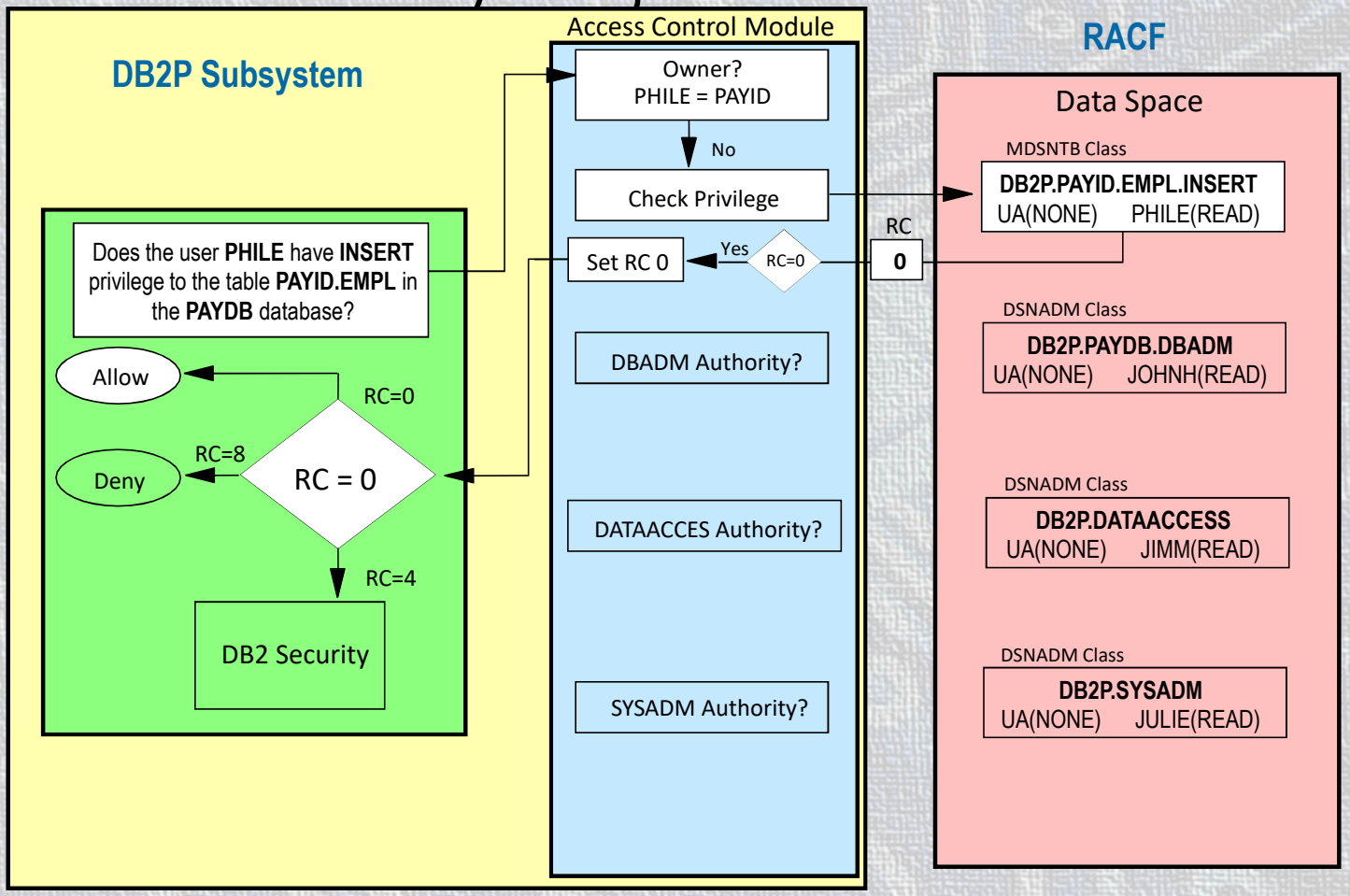
Access Allowed By Ownership





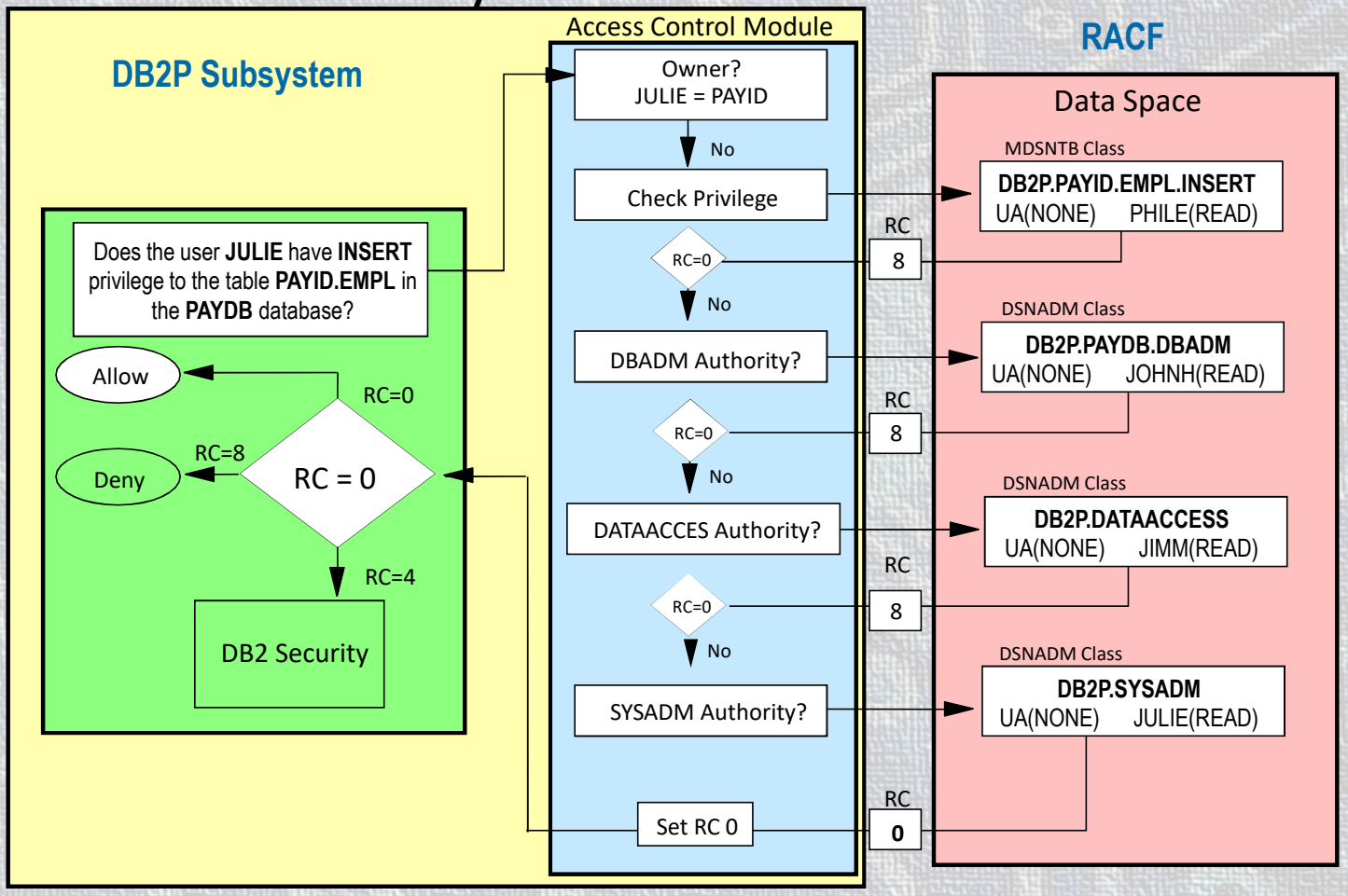
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Access Allowed By Object Profile



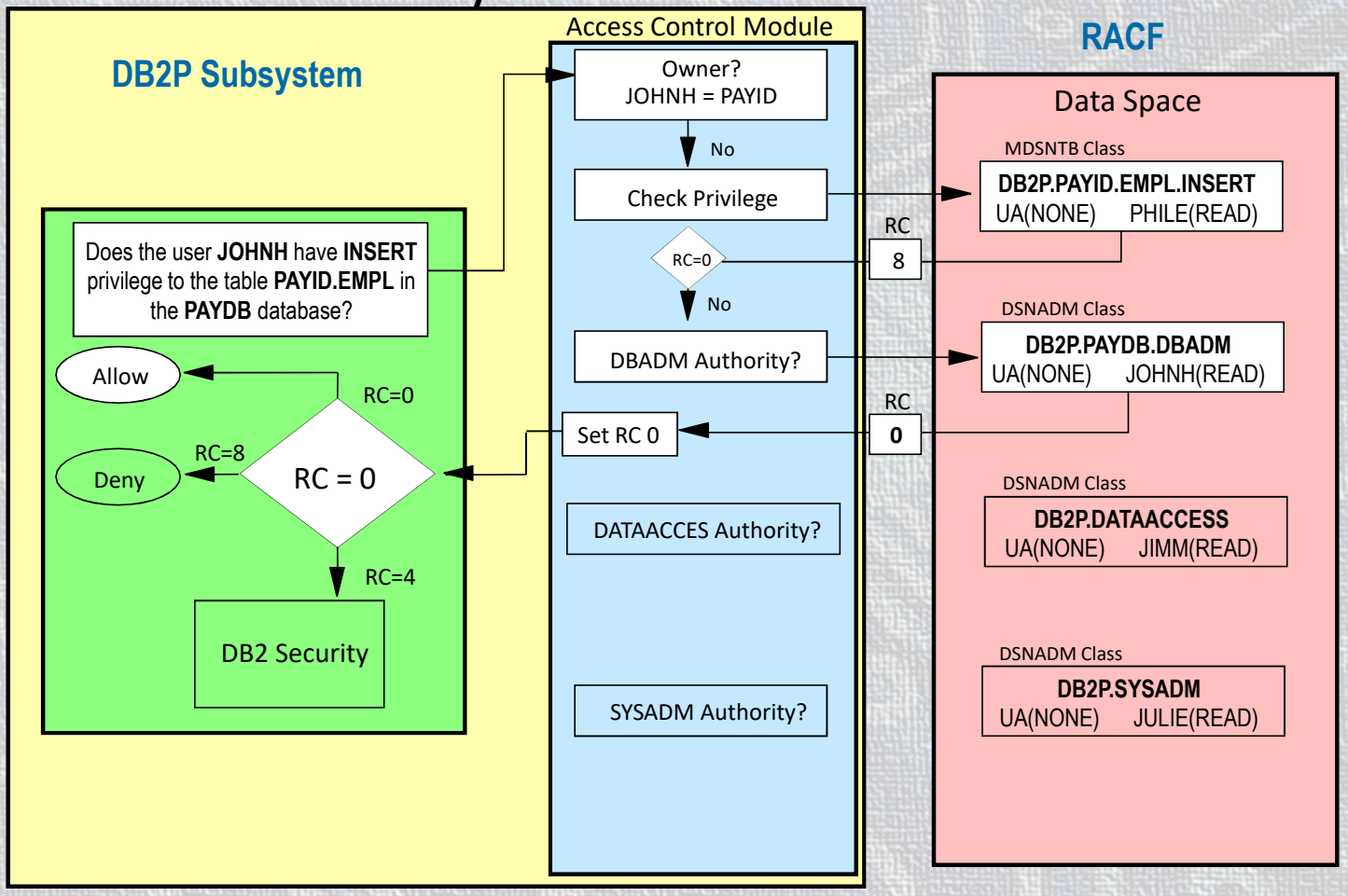
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Access Allowed By SYSADM Profile



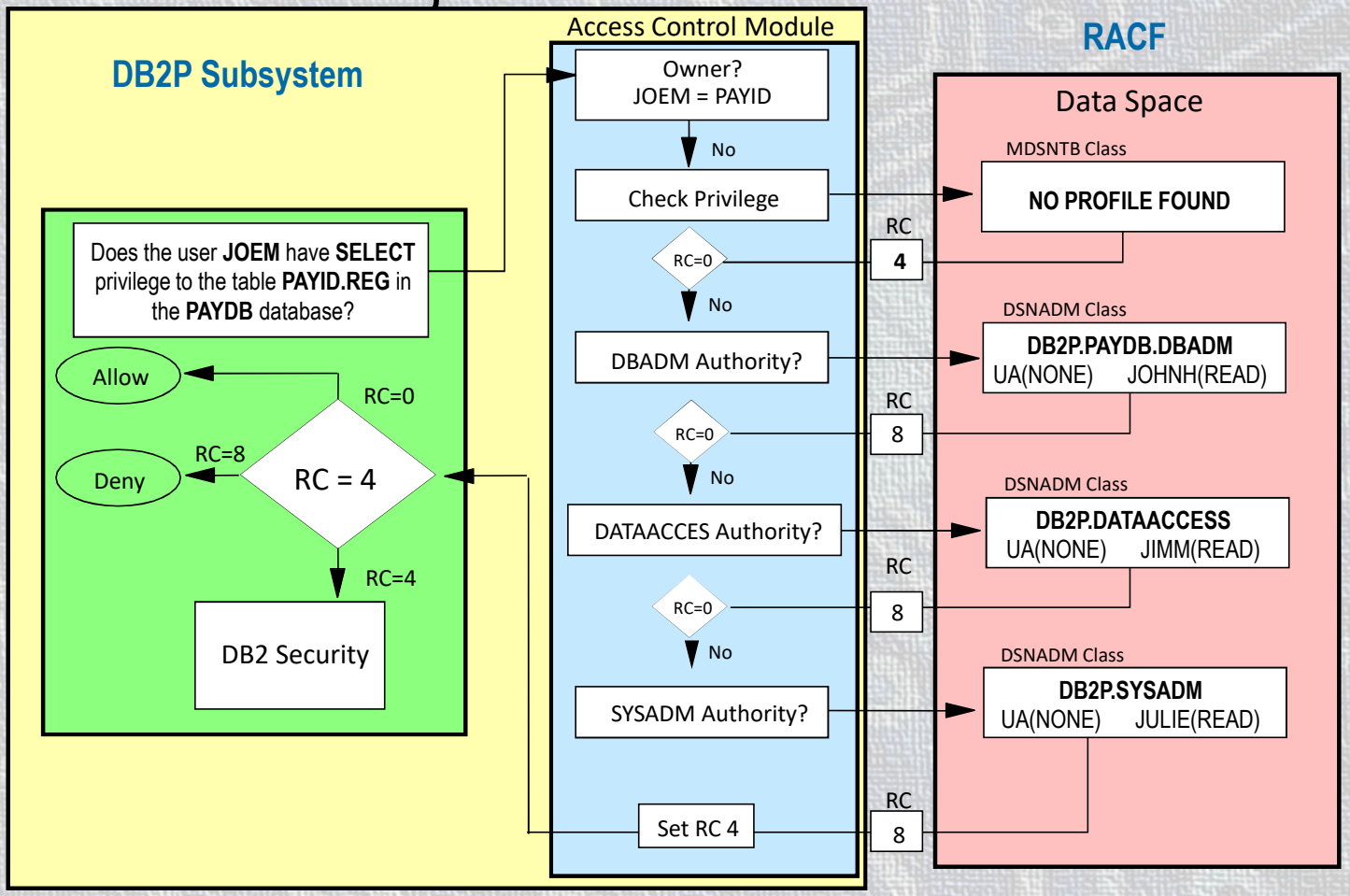
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Access Allowed By DBADM Profile



VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Unprotected Object - Defer To DB2



DB2 Access Events Logged to SMF

Violations

- RACF has checked all object profiles
- 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

Migrating from DB2 Security to RACF Security

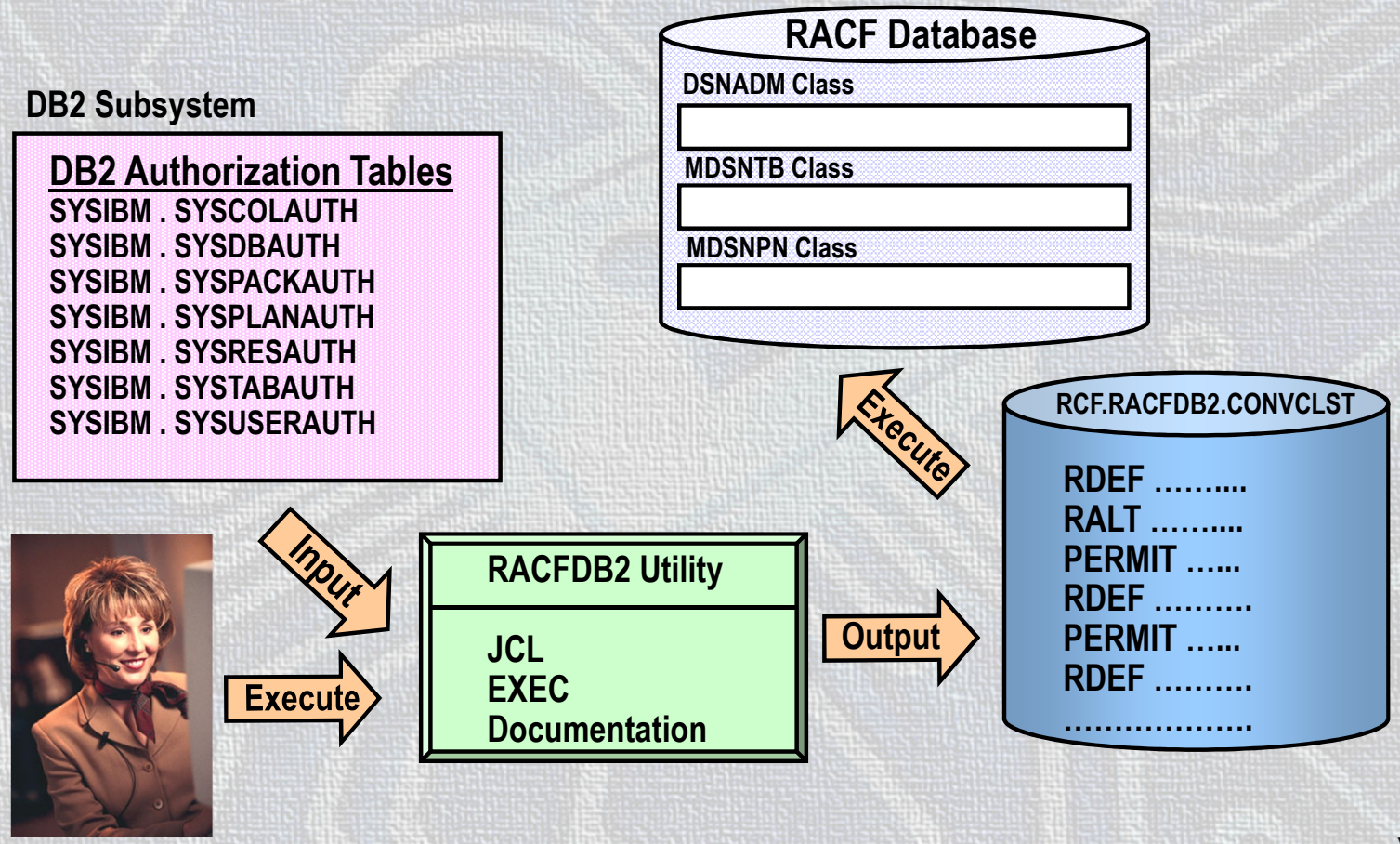
Migrating from DB2 to RACF Security

How can I convert from DB2 security to RACF security?

Let's use the DB2 to RACF Migration Utility!

RACF/DB2 Migration Utility

DB2 to RACF Migration Tool



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Running the RACFDB2 Utility

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

Migration to RACF Security

- RACF commands are generated for only 9 of the 16 DB2 Object types, and DB2 Authorities
- Not all DB2 Object types are handled:
  - Global Variables
  - Java Archive files (JARs)
  - Schemas
  - Sequences
  - Stored Procedures
  - User Defined Distinct Types
  - User Defined Functions
  - Trusted Context
- Privileges higher than SELECT to a VIEW not processed correctly

Profiles Generated by RACFDB2 Utility

- Builds RDEFINE commands for all objects, privileges and authorities
- AUDIT(ALL(READ)) is set for DB2 administrative authorities
- UACC is set to READ if granted to PUBLIC
- PERMIT with ACCESS(READ) if authorized without GRANT
- PERMIT with ACCESS(ALTER) if authorized with GRANT
- All profiles are defined in member classes

Executing the Commands Generated

- Consider replacing many discrete profiles!
  - Use generic profiles?
  - Use some grouping profiles?
  - Use RACFVARS variable?

- Execute the generated RACF commands
- Customize the DSNX@XAC exit
- Activate the DB2 general resource classes
- Activate the DSNX@XAC exit
- Administer DB2 security with RACF

Considerations

- **Any tools that use the security tables in DB2 catalog?**
- **There are some differences between DB2 and RACF security**
  - See *DB2 UDB RACF Access Control Module Guide*
  - BINDAGENT (see next slide)
  - “Any table” privilege
  - WITH GRANT OPTION

BINDAGENT

- Beginning in DB2 V11 BINDAGENT has been fixed
- You must use a new DSNZPARM
  - AUTHEXIT_CHECK=DB2 (the default is AUTHEXIT_CHECK=PRIMARY
  - Specifies that Db2 provides the ACEE of the package or plan owner to perform authorization checking when processing the autobind, BIND and REBIND commands
- Assume JIMTEST will BIND Plans on behalf of JIMM
  - Create [ssid].JIMM.BINDAGENT in the MDSNSM class (or user defined class)
  - Permit JIMTEST read access to the profile
  - JIMTEST does a BIND specifying OWNER(JIMM)
  - The OWNER may be a GROUP

Questions

How to Contact Us

Vanguard Integrity Professionals
6625 South Eastern Ave., Suite 100
Las Vegas, NV 89119-3930

Direct/International: (702) 794-0014
Toll Free: (877) 794-0014
info@go2vanguard.com

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS