VANGUARD
Integrity Professionals
Enterprise Security Software

Considerations for Migrating DB2 Security to RACF

SHARE 121 – Boston, MA
Session 14015
August 11 - 16, 2013

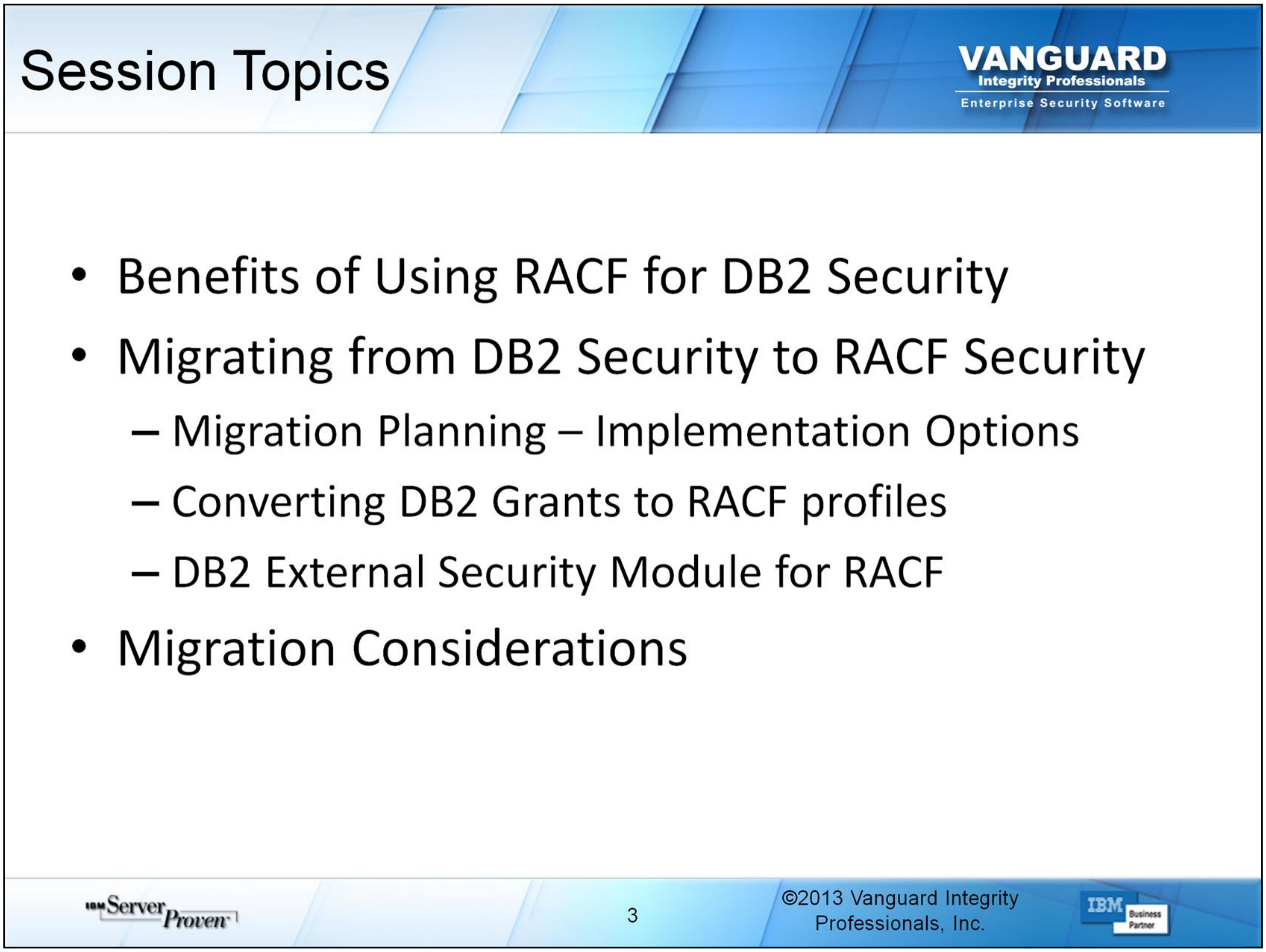
Phil Emrich
Sr. Professional Services Consultant
pemrich@go2vanguard.com
+1-702-234-8495

IBM Server Proven

IBM Business Partner

Trademarks

- IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, or service names may be trademarks or service marks of others.



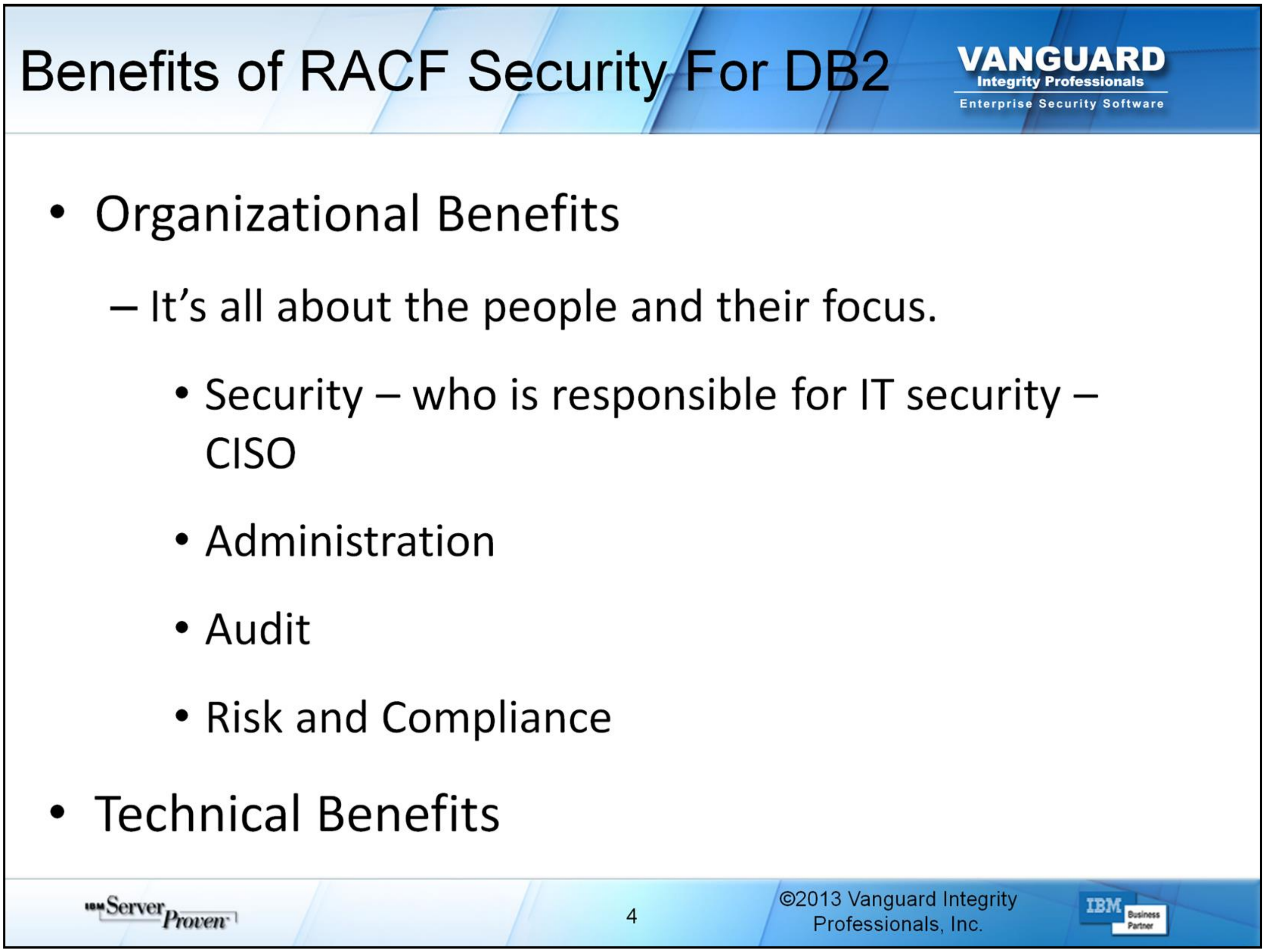
Session Topics

- 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

3

This session is devoted to a discussion of the advantages and considerations that should be considered when contemplating or proposing a migration of security for DB2 from the security mechanisms internal to DB2 itself to security for DB2 based on profiles defined in a RACF database.

Other presentations presented at SHARE and GSE in Europe have gone into greater detail on the technical mechanisms by which security using RACF for DB2 is achieved.. In the vast majority of situations identical security will be provided, but there are a number of specific instances where there are differences in the security provides. It is not necessarily true in these cases that the security is less robust when using RACF, but simply or subtly different.



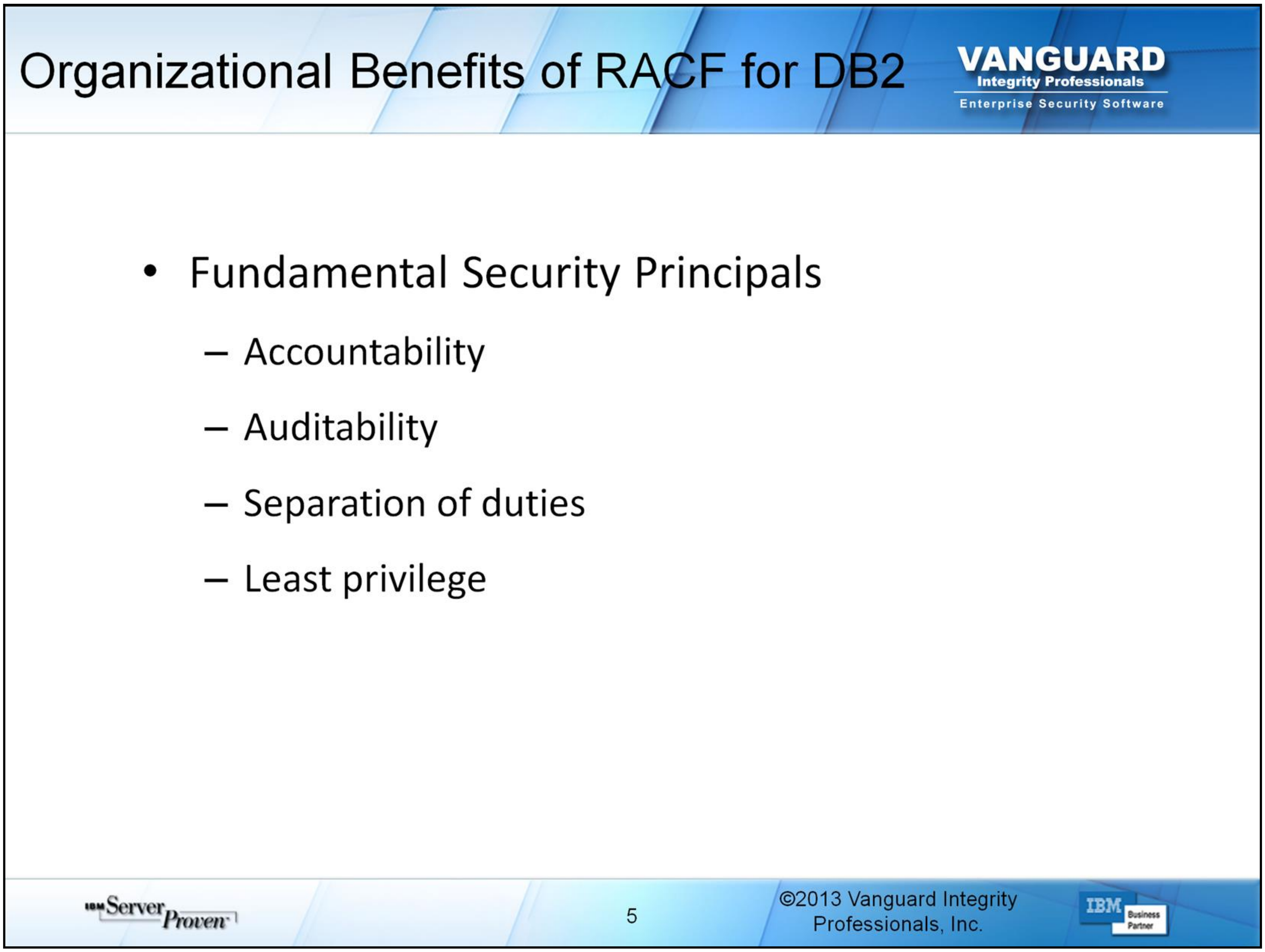
Benefits of RACF Security For DB2

- Organizational Benefits
  - It’s all about the people and their focus.
    - Security – who is responsible for IT security – CISO
    - Administration
    - Audit
    - Risk and Compliance
- Technical Benefits

The are two primary areas in which potential benefits can be derived from the use of RACF for DB2 security. The first of these are what I’ve chosen to call “organizational” benefits. The second area, technical benefits, have to do with the constructs used to implement security controls and the greater flexibility that RACF offers.

The organizational benefits have a number of aspects, but basic to them is the role of the individuals implementing the security controls and performing the ongoing administration of those controls. In most organizations in which the internal DB2 mechanisms are in use the implementation and administration is most commonly performed by a DB2 technician, either a DB2 systems programmer, DB2 database administrator (DBA), or an individual whose responsibilities encompass both of those roles. While it’s likely that these individuals are technically competent, it’s equally likely that implementing robust security is a lower priority than their efforts to address the other aspects of their responsibilities.

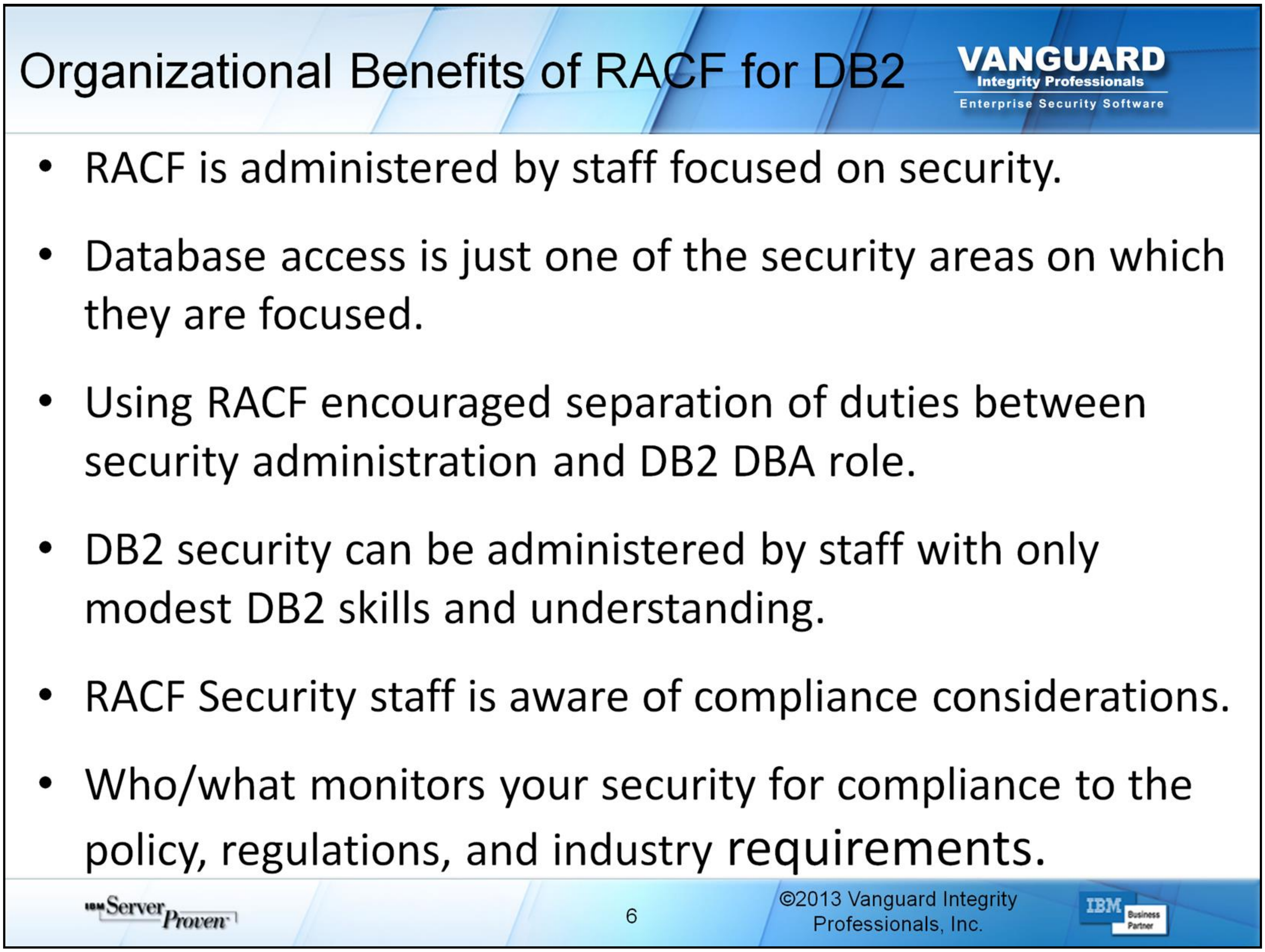
The CISO and the staff the reports to that individual, on the other had are primarily focused on security and risk management, not just for database content or DB2 specifically but for all aspects of security that affect the organization.



Organizational Benefits of RACF for DB2

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

These fundamental security principals guide the implementation and activities of the staff responsible for security within almost any organization.



Organizational Benefits of RACF for DB2

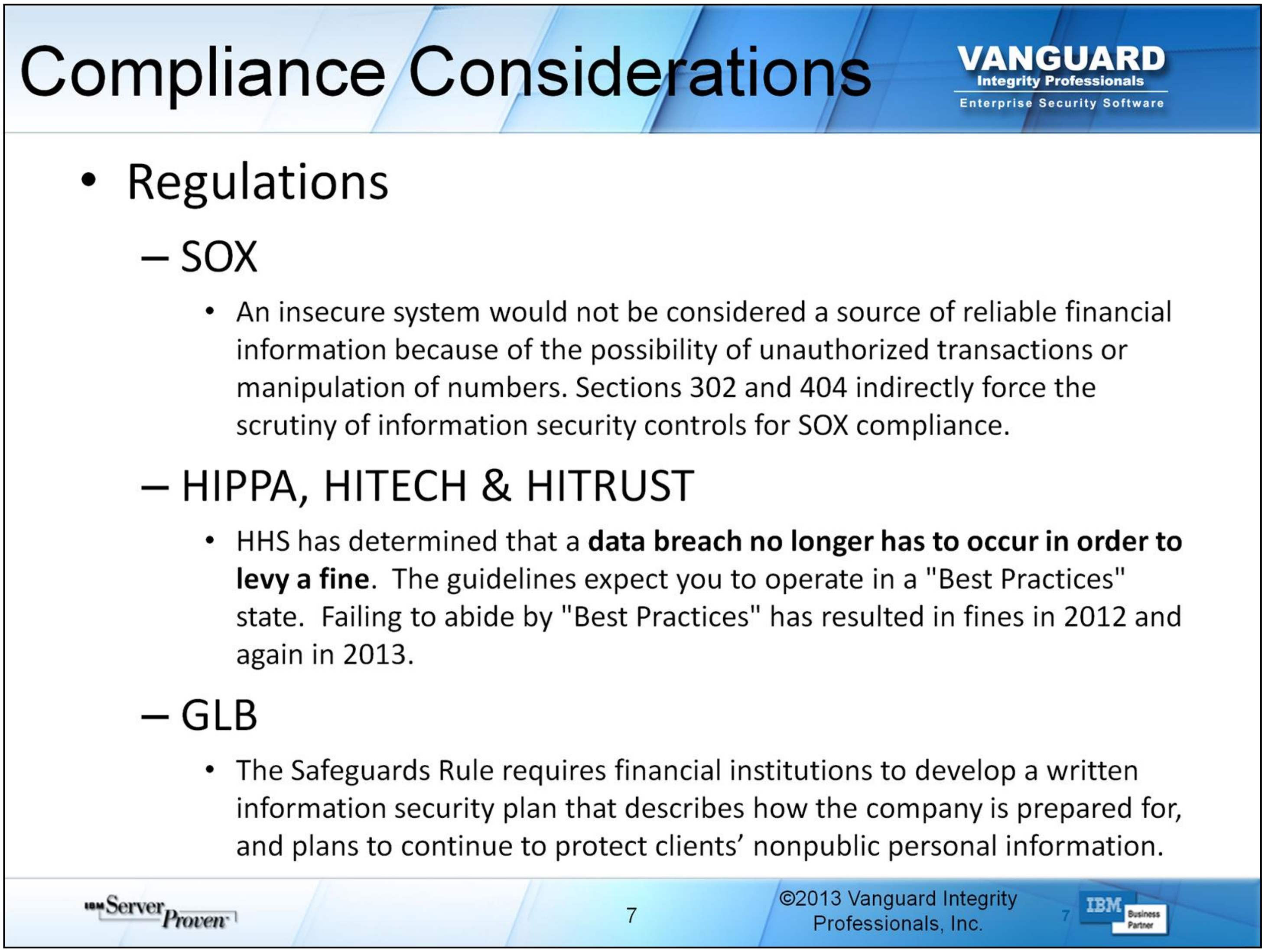
- RACF is administered by staff focused on security.
- Database access is just one of the security areas on which they are focused.
- Using RACF encouraged separation of duties between security administration and DB2 DBA role.
- DB2 security can be administered by staff with only modest DB2 skills and understanding.
- RACF Security staff is aware of compliance considerations.
- Who/what monitors your security for compliance to the policy, regulations, and industry requirements.

Here are some typical examples of the perspective, activities, and responsibilities of the staff responsible for security within many organizations.

RACF is, if not the only security software, for use on z/OS platforms is the primary software for implementing and controlling access to z/OS platform resources for the majority of resource manager software and is generally managed by a team focused on security for z/OS or for the enterprise as a whole.

The primary role of DBAs or DB2 systems programmers is to provide access to data; while the primary role of security staff is to limit access to data. DB2 SECADM introduced in DB2 V10 improves the possibility of introducing “separation of duties” within DB2, but is not automatic. You have to redesign the responsibilities of individuals within the DB2 technical staff to achieve it, but you would still not likely have a separate reporting path.

This team, extending to all of the individuals who are responsible to the CISO, are primarily concerned with security, and not only related considerations such as compliance with internal corporate security related policies, but also compliance with governmental regulations and industry requirements and guidelines.



Compliance Considerations

- Regulations
  - SOX
    - An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or manipulation of numbers. Sections 302 and 404 indirectly force the scrutiny of information security controls for SOX compliance.
  - HIPPA, HITECH & HITRUST
    - HHS has determined that a **data breach no longer has to occur in order to levy a fine**. The guidelines expect you to operate in a "Best Practices" state. Failing to abide by "Best Practices" has resulted in fines in 2012 and again in 2013.
  - GLB
    - The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information.

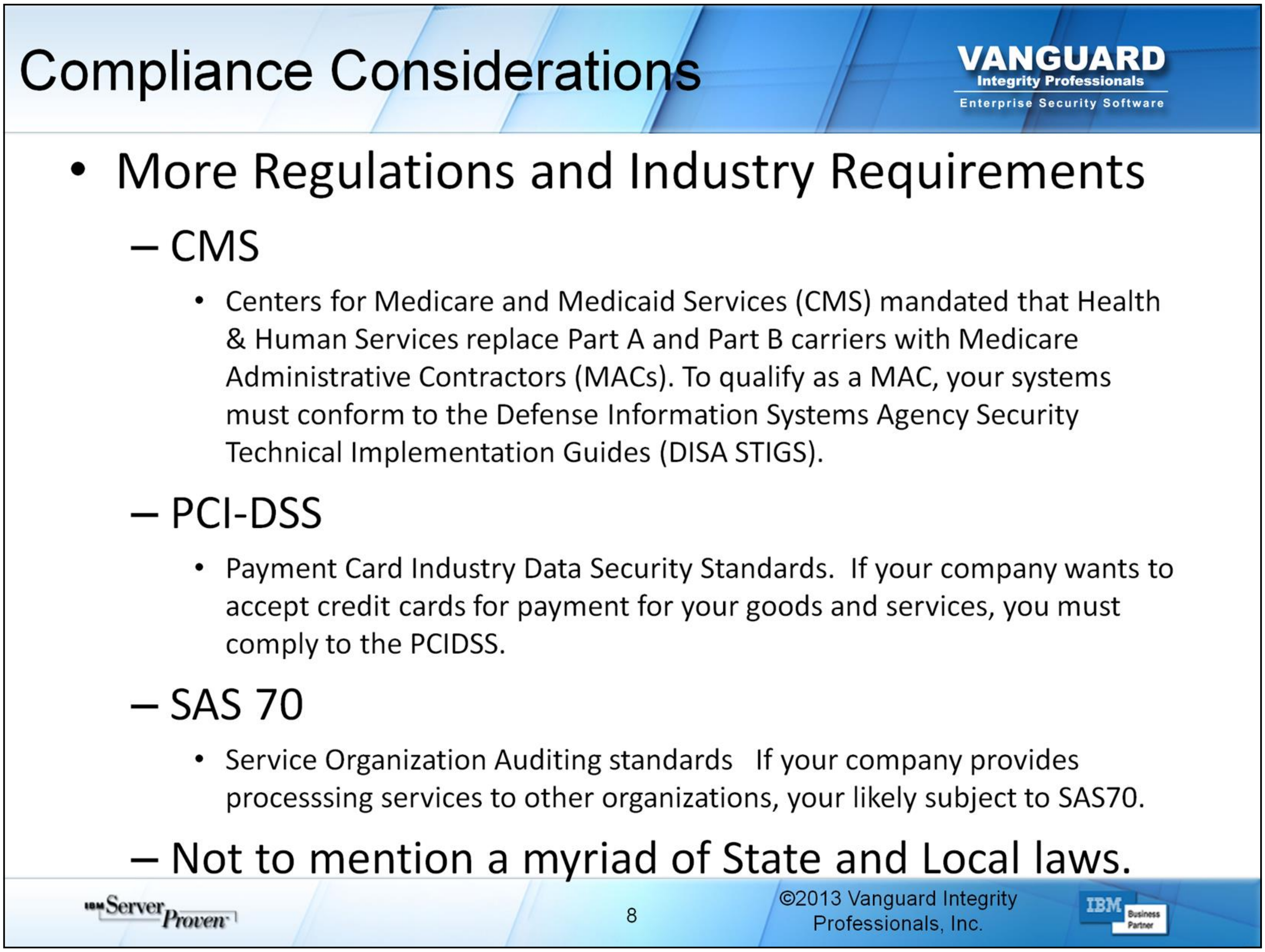
Depending on the particular situation of an individual organization here are just a few of the regulations with which an organization may be required to comply.

SOX – Sarbanes, Oxley - applicable to publicly traded companies

HIPAA, HITECH, & HITRUST – applicable to the health care and health insurance industries

GLB – Gramm–Leach–Bliley – applicable to financial services companies

Many organizations are subject to mulitple sets of regulatory requirements.



Compliance Considerations

VANGUARD Integrity Professionals
Enterprise Security Software

- More Regulations and Industry Requirements
  - CMS
    - Centers for Medicare and Medicaid Services (CMS) mandated that Health & Human Services replace Part A and Part B carriers with Medicare Administrative Contractors (MACs). To qualify as a MAC, your systems must conform to the Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGS).
  - PCI-DSS
    - Payment Card Industry Data Security Standards. If your company wants to accept credit cards for payment for your goods and services, you must comply to the PCIDSS.
  - SAS 70
    - Service Organization Auditing standards   If your company provides processsing services to other organizations, your likely subject to SAS70.
  - Not to mention a myriad of State and Local laws.

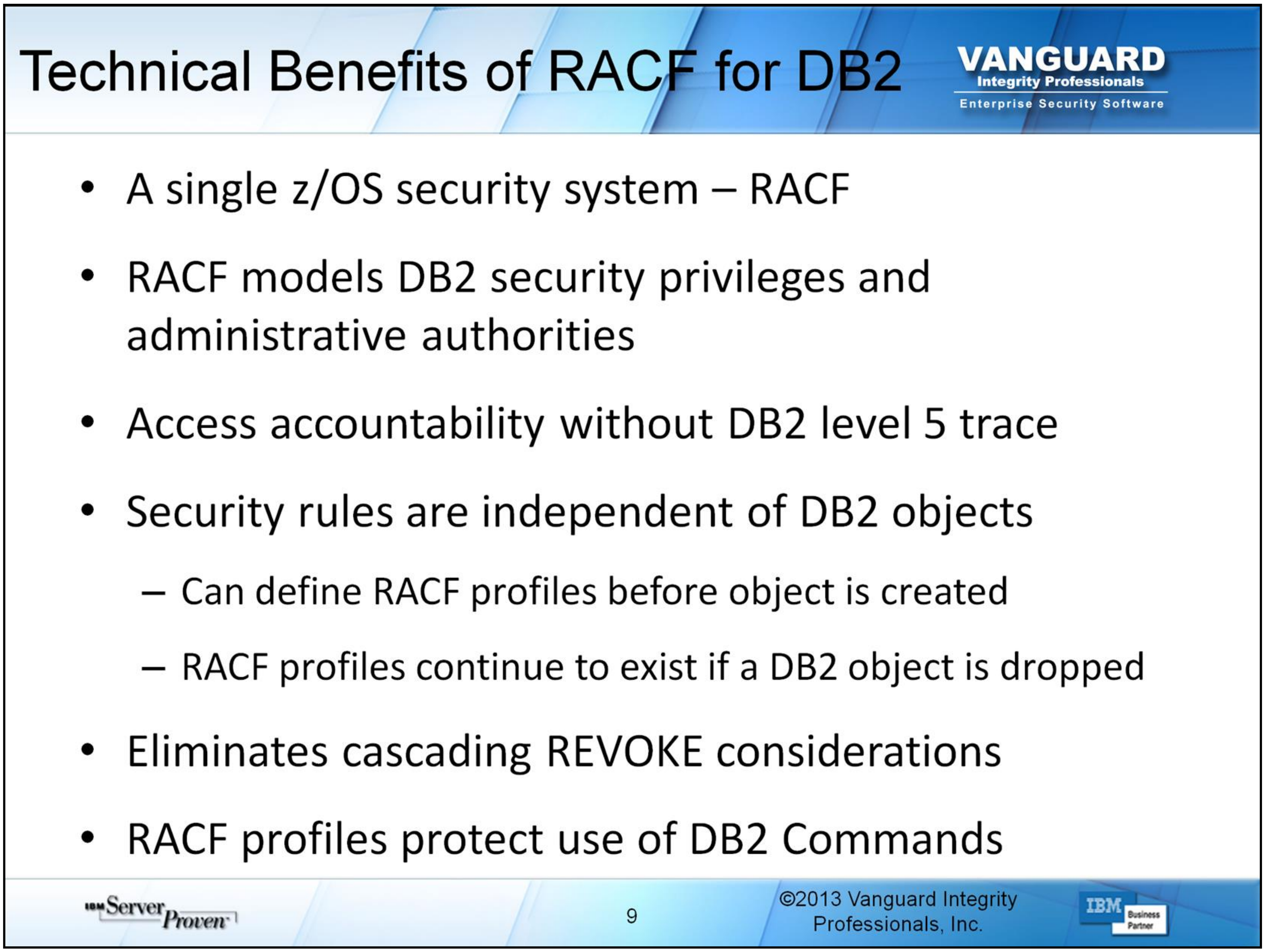
8

Medicare Authorized Contractors (MACs) are just one type of organization that is required to comply with the Security Technical Implementation Guidelines (STIGs) published by NIST for the z/OS platform. All organizations within the U.S. Federal government utilizing z/OS platforms are required to comply with these documented standards.

An even broader cross-section of organizations, both within and outside of the United States, are affected by the Payment Card Industry Data Security Standards (PCI-DSS) and the impact on the security that this standard imposes for z/OS platforms thst are “in scope”, processing or storing data related to credit card transactions.

SAS 70 is a set of auditing standards to which many organizations are subject when they provide services to other organizations. Since security is only as good as “the weakest link” organizations desire assurance that their business partners are reasonably secure.

Adding even more complexity to the challenge of complying with both federal regulatory and industry requirements is the challenge of complying with regulations adopted by various states that may well apply to organizations who do business with residents of a particular state, even if the organization has no premises with that state. At present, 46 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have security breach laws.



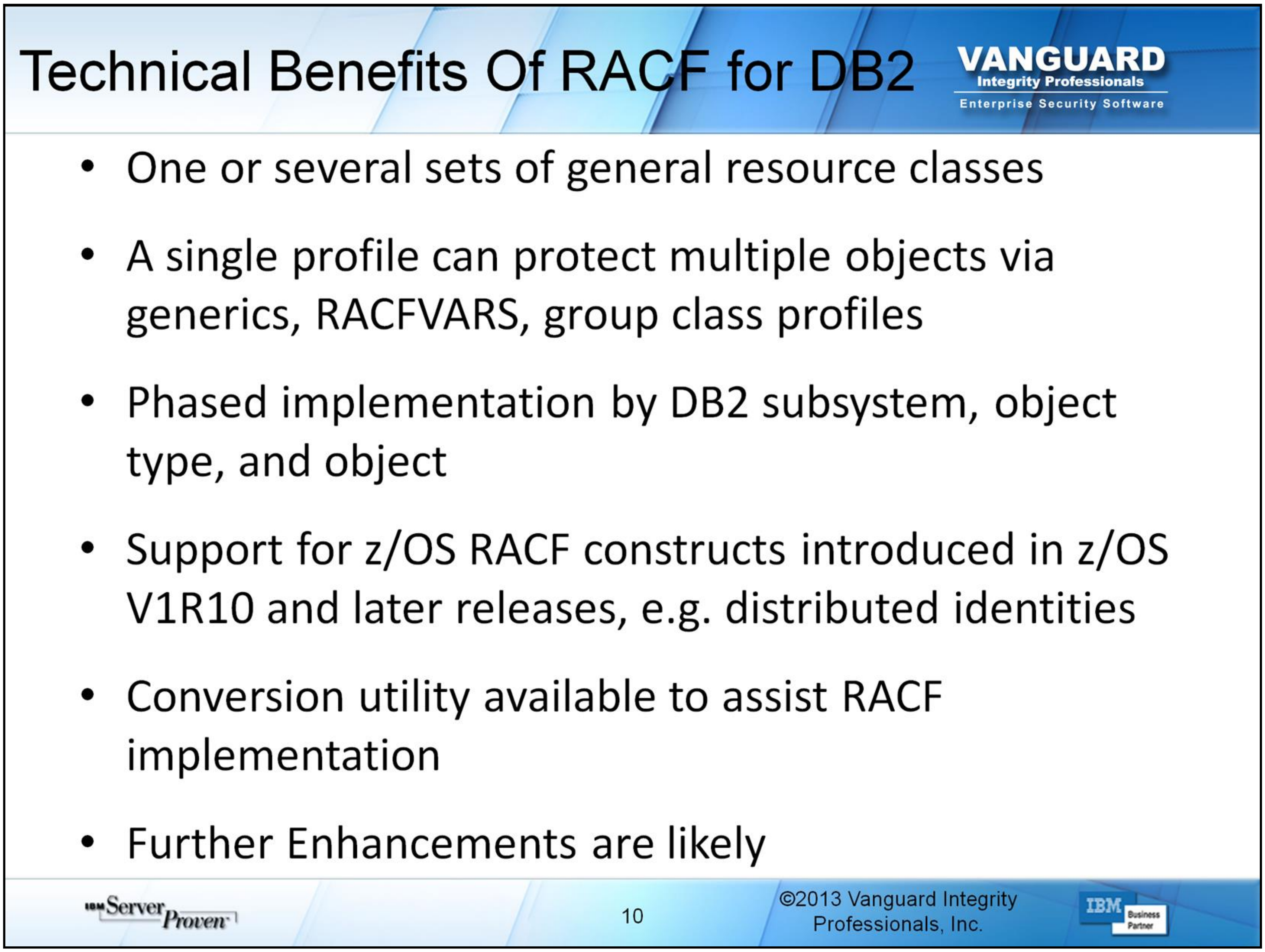
Technical Benefits of RACF for DB2

- A single z/OS security system – RACF
- RACF models DB2 security privileges and administrative authorities
- Access accountability without DB2 level 5 trace
- Security rules are independent of DB2 objects
  - Can define RACF profiles before object is created
  - RACF profiles continue to exist if a DB2 object is dropped
- Eliminates cascading REVOKE considerations
- RACF profiles protect use of DB2 Commands

Over the long history of mainframe software many components and products have provided mechanisms to control access to the resouces they manage. But of the past decade or two many of the resource managers on the z/OS platform have moved to support a SAF or RACF interface for implementing those resource access controls, either replacing their own internal mechanisms or offering them as an option for organizations that wish to use a single facility for managing security across all the z/OS resource managers.

DB2 development began the process of offering RACF as an alternative to its own internal security mechanisms in DB2 V6 in the late 1990s approximately fifteen years ago and has improved the capabilities for managing security for DB2 objects using RACF in almost every release since, in a number of instances in parallel with enhancements to the internal DB2 mechanisms.

This visual introduces a number of the characteristics for managing security for DB2 objects through RACF that have advantages over the internal DB2 security facilities.

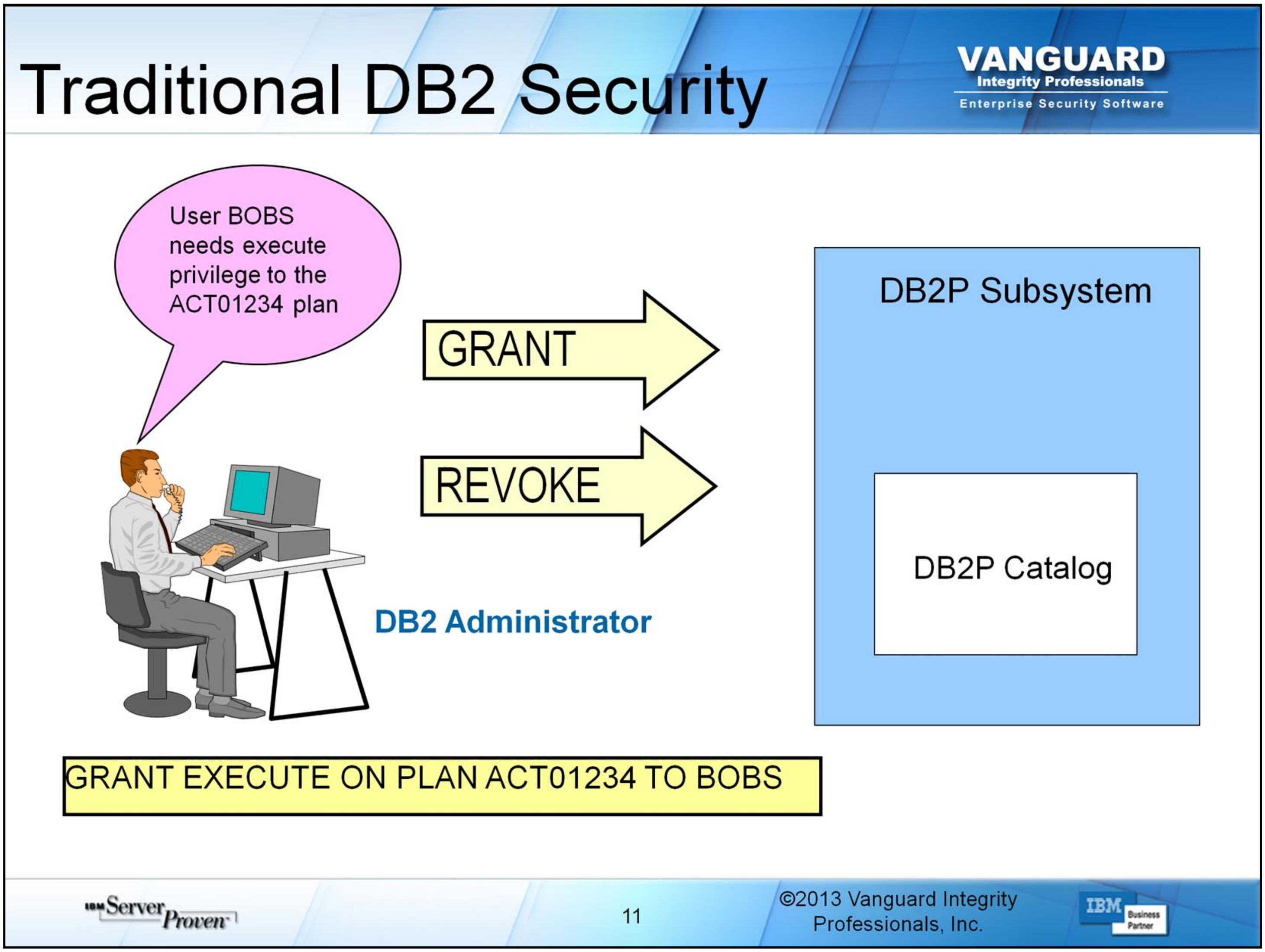


Technical Benefits Of RACF for DB2

- 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 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

This visual introduces a number of additional characteristics for managing security for DB2 objects through RACF that have advantages over the internal DB2 security facilities.

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

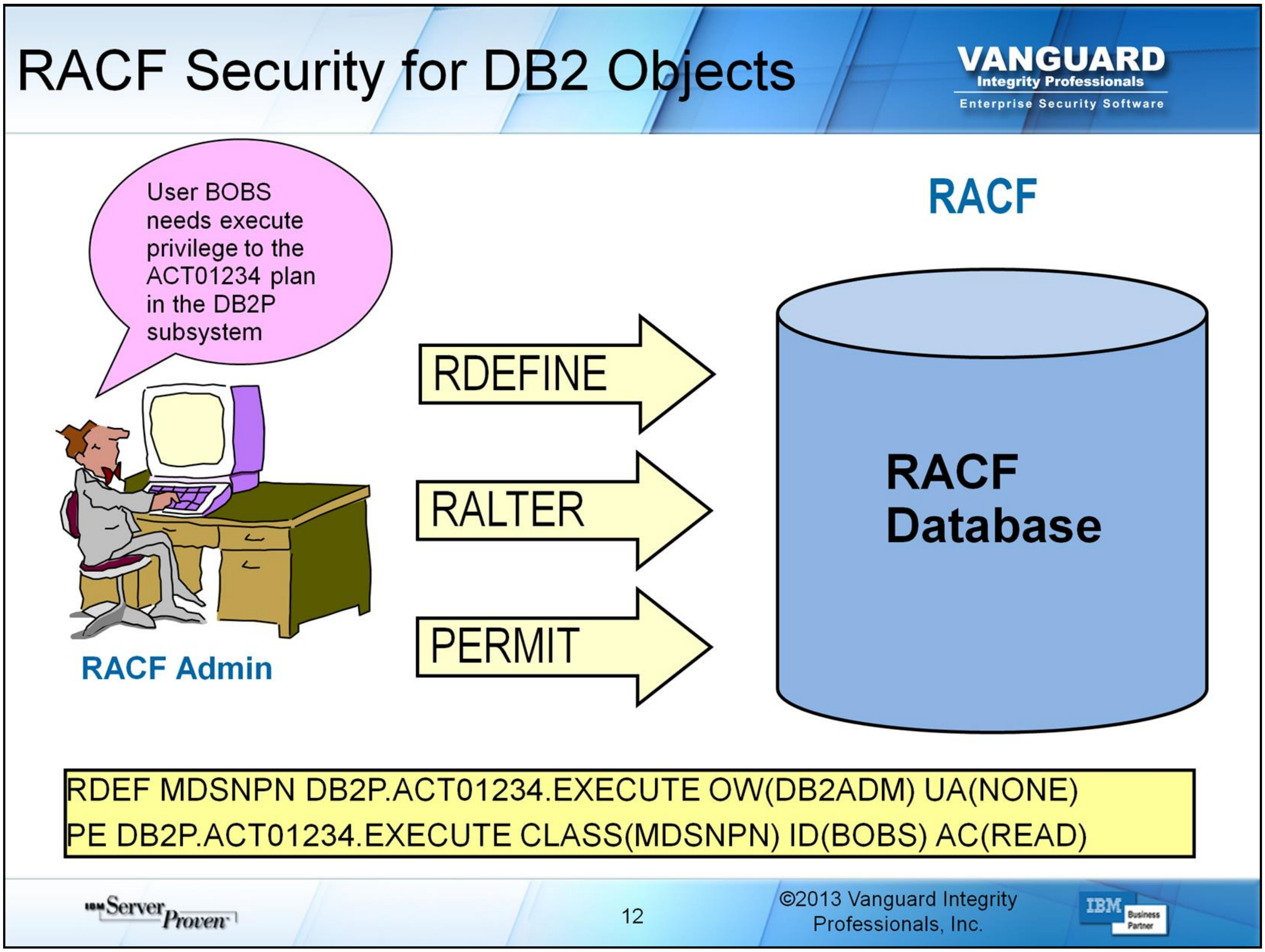
The DB2 catalog is a collection of tables that contains data about everything defined to DB2.

Each DB2 subsystem has its own set of catalog tables.

Security catalog tables are a part of the DB2 catalog. They contain information about the privileges held by Ids.

The SQL statements GRANT and REVOKE are used to administer security for DB2 objects.

Only IDs with SYSADM and SYSCTRL authority are automatically privileged to retrieve information from the catalog tables.



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

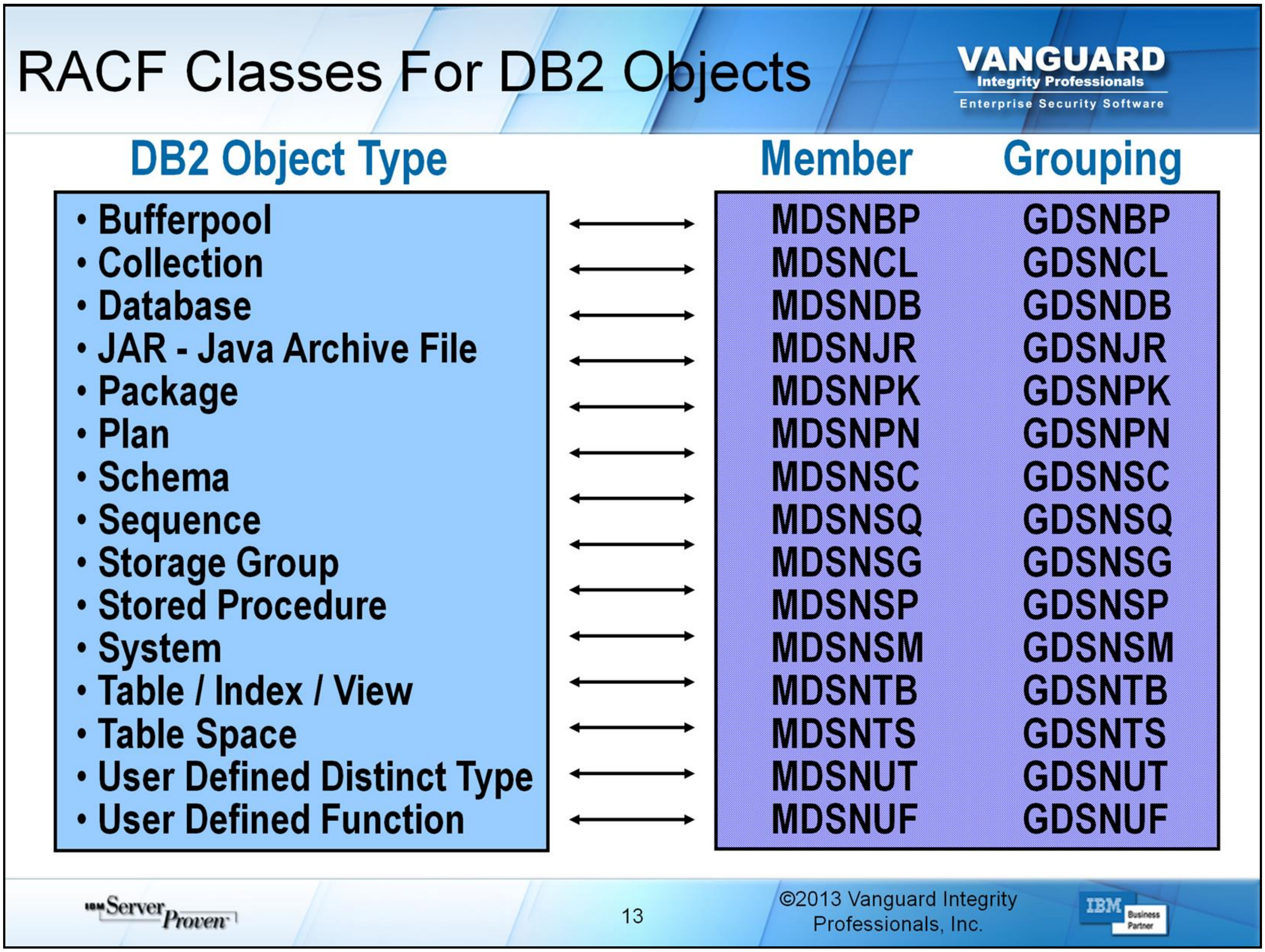
```
RDEF MDSNPN DB2P.ACT01234.EXECUTE OW(DB2ADM) UA(NONE)
PE DB2P.ACT01234.EXECUTE CLASS(MDSNPN) ID(BOBS) AC(READ)
```

RACF Security for DB2 Objects:

- RACF profiles can be used to control access to DB2 objects
- RACF profiles can be used to give DB2 administrative authorities to users
- If a RACF profile does not exist, then the access decision is handled by DB2

RACF/DB2 security gives the RACF administrator the ability to:

- Validate auth IDs before granting DB2 authorities
- Define security rules before the object is created
- Eliminate the ability to define duplicate security rules
- Preserve security rules for dropped objects
- Separate Control rights from Access rights
- Administer DB2 security with a minimum of DB2 skill



RACF Classes For DB2 Objects

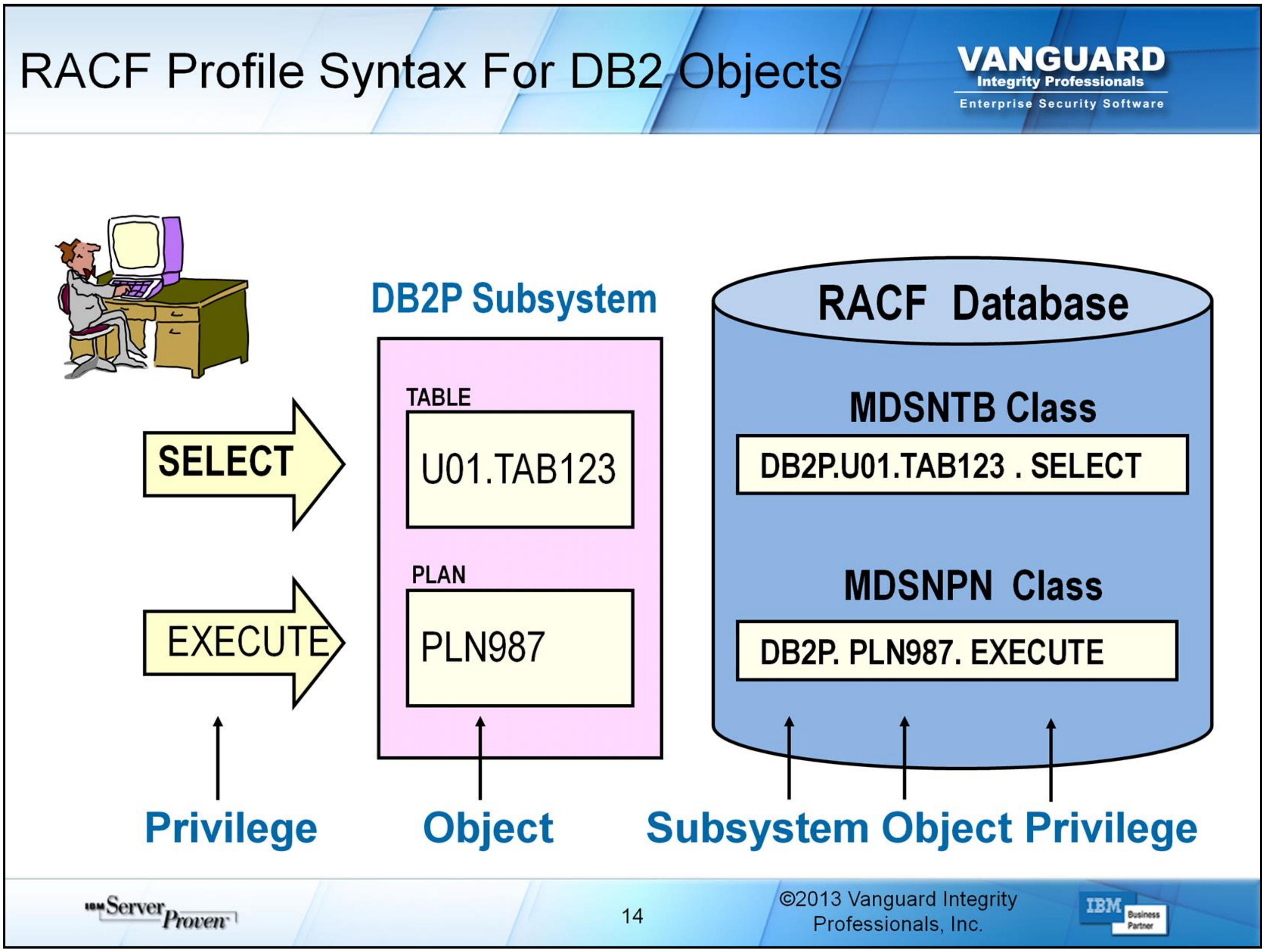
DB2 Object Type	Member	Grouping
Bufferpool	MDSNBP	GDSNBP
Collection	MDSNCL	GDSNCL
Database	MDSNDB	GDSNDB
JAR - Java Archive File	MDSNJR	GDSNJR
Package	MDSNPK	GDSNPK
Plan	MDSNPN	GDSNPN
Schema	MDSNSC	GDSNSC
Sequence	MDSNSQ	GDSNSQ
Storage Group	MDSNSG	GDSNSG
Stored Procedure	MDSNSP	GDSNSP
System	MDSNSM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

For each type of DB2 object, RACF provides a pair of general resource classes.

- The naming convention:
  - –M is for member class
  - –G is for grouping class
  - –DSN is the DB2 subsystem name
  - –The last two characters indicate the type of object

The classes shown here are the default classes which are already in the RACF class descriptor table and RACF router table.

You can define other installation-defined classes, but you will have to add them to the RACF class descriptor and router tables.



RACF Profile Syntax For DB2 Objects

A pair of RACF general resource classes correspond to each kind of DB2 object. The RACF profile name defines the DB2 object.

The privilege granted by the profile is the last qualifier of the profile name.

We grant the privilege to a user by giving READ access in the profile.

In the example shown here:

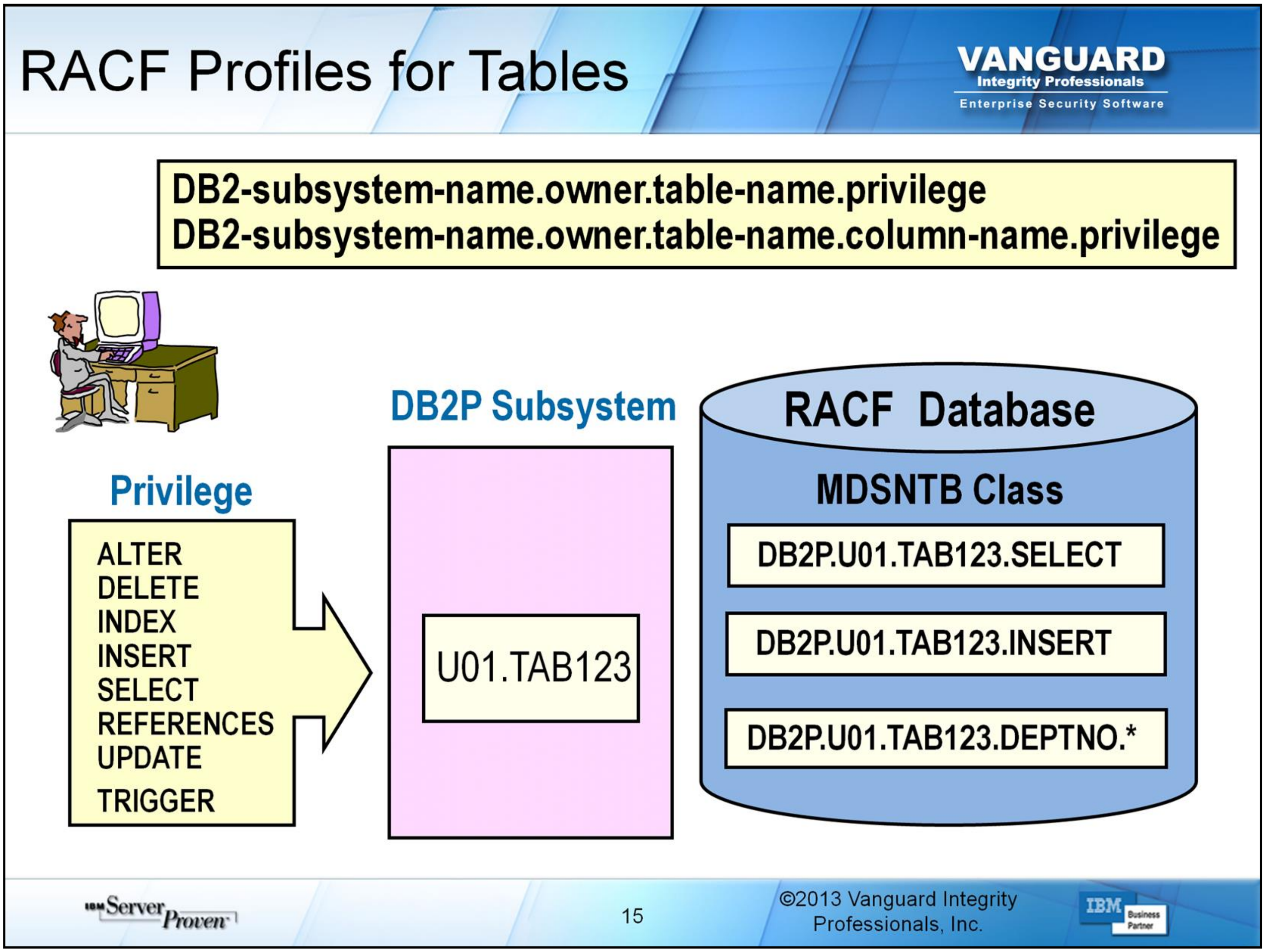
MDSNTB is the general resource member class for DB2 tables

MDSNPN is the general resource member class for DB2 plans

DB2P is the name of the DB2 subsystem

TAB123 is a DB2 table that is owned by the U01 ID

PLN987 is a DB2 plan



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.*

The MDSNTB and GDSNTB general resource classes are used to control access to DB2 tables.

- The first qualifier is the DB2 subsystem name
- The last qualifier is the privilege name

The table name is made up of two qualifiers:

- The first qualifier is the owner of the table
- The second qualifier is the table name

If the profile covers only a specific column in the table, then the next-to-last qualifier is the column name

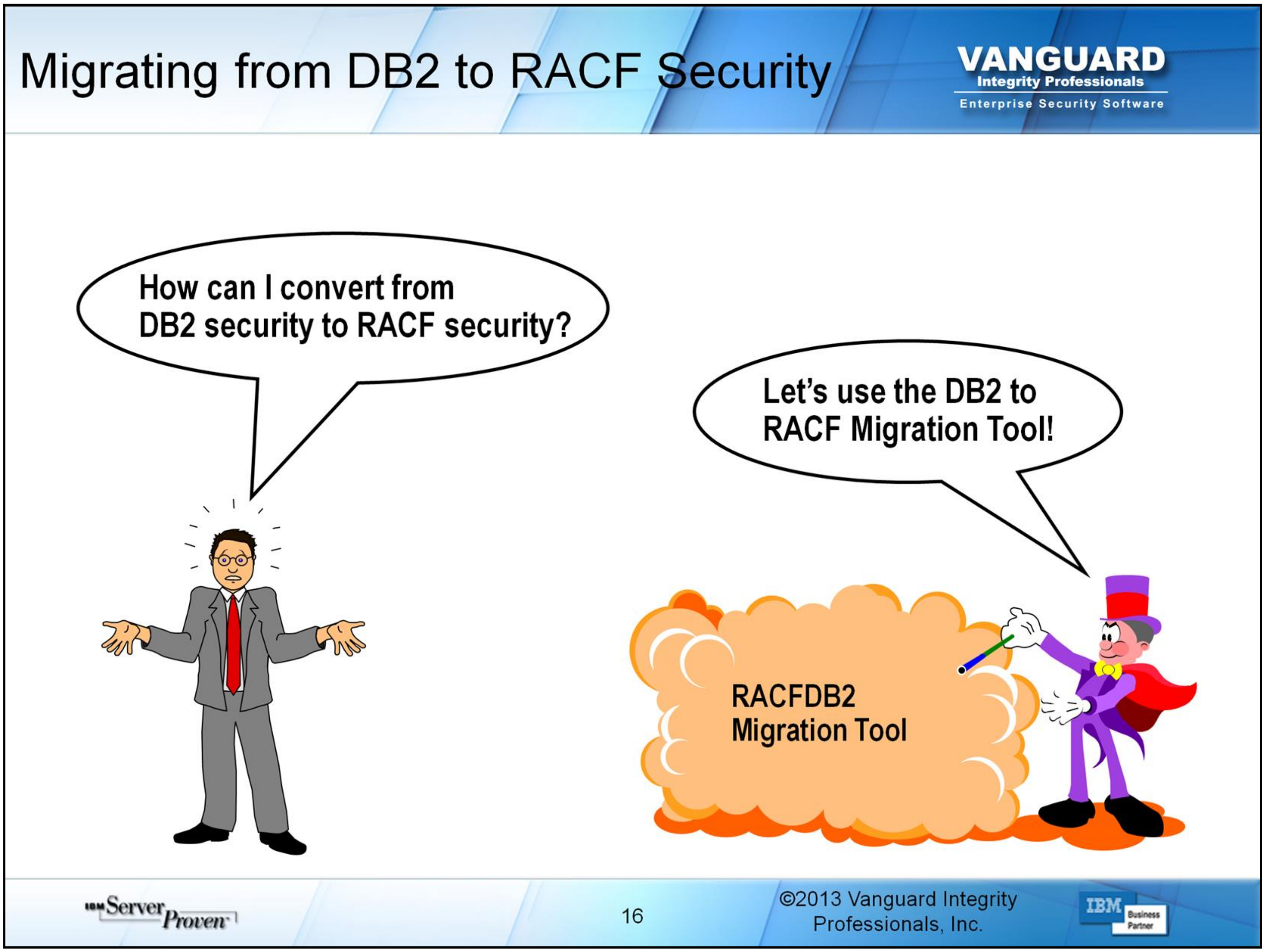
In the examples:

- The first profile covers the SELECT privilege for table TAB123 which is owned by the U01 id
- The second profile covers the INSERT privilege for table TAB123
- The third profile covers all privileges for the DEPTNO column of table TAB123

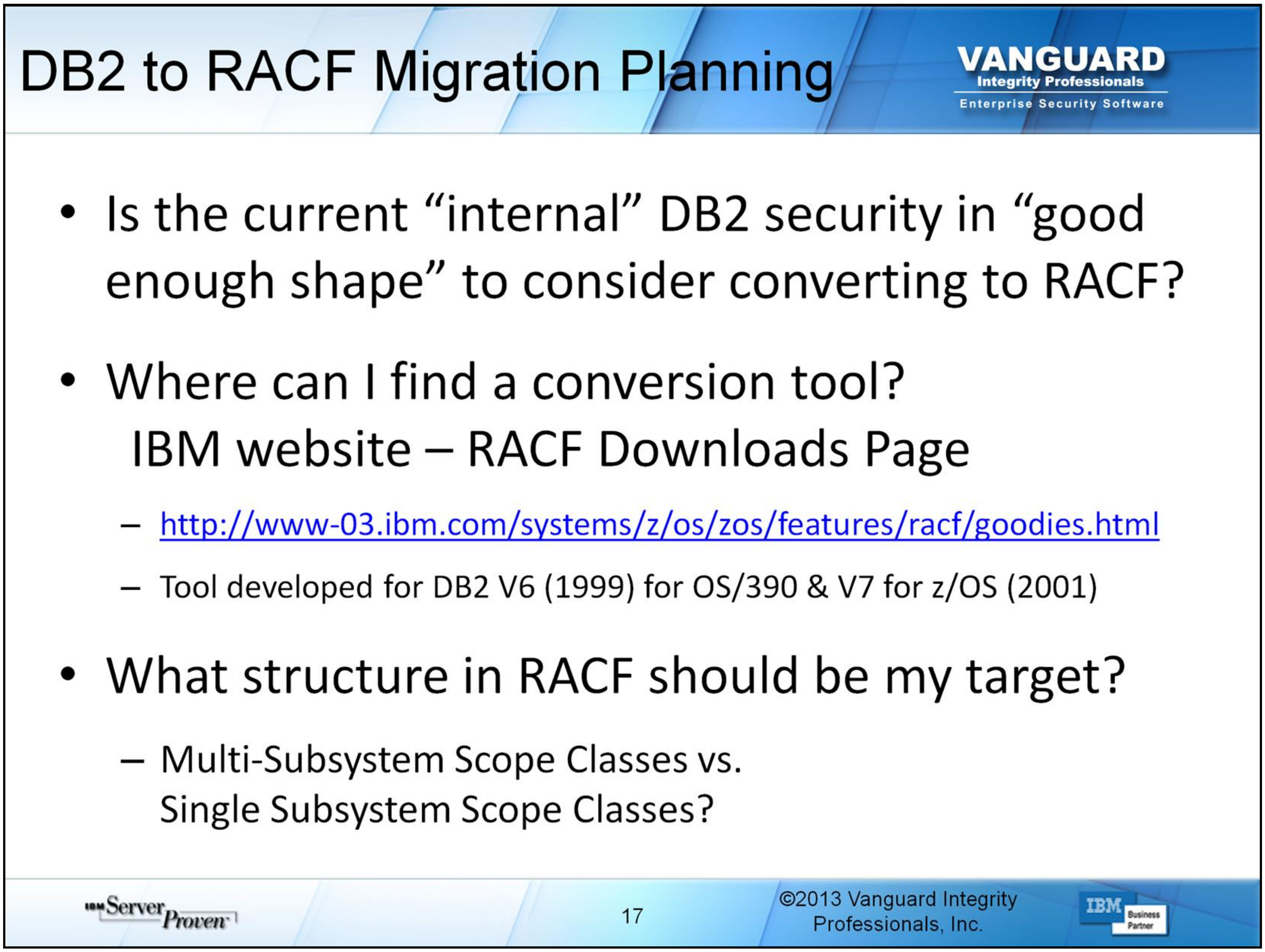
If a user does not have access to the table, DB2 calls RACF again to check for access to the column.

Migrating from DB2 to RACF Security

VANGUARD
Integrity Professionals
Enterprise Security Software


How can I convert from DB2 security to RACF security?
Let's use the DB2 to RACF Migration Tool!
RACFDB2 Migration Tool

- A utility to help migrate from DB2 security to RACF security is available from IBM.
- This utility is available at no charge from IBM on the Internet, downloadable for the RACF Downloads page on the IBM web site.
- The utility generates RACF commands that are equivalent to the DB2 security defined in the DB2 authorization tables.



DB2 to RACF Migration Planning

VANGUARD Integrity Professionals
Enterprise Security Software

- 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?

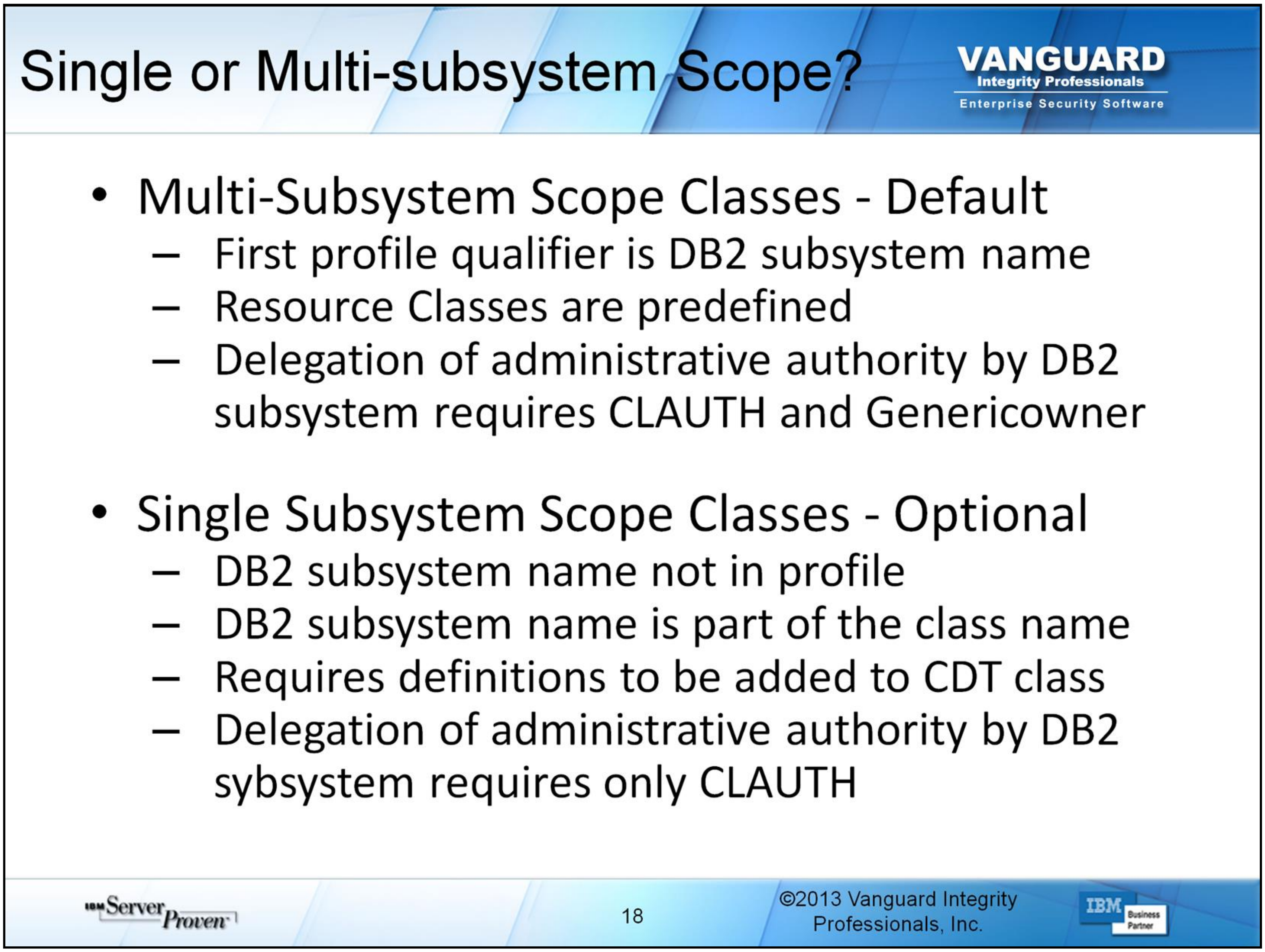
IBM Server Proven

IBM Business Partner

Before embarking on a conversion of existing DB2 authorization table content to RACF you must first do some analysis to determine whether the security as currently defined is at least approximately what you would like to have in place after the conversion as measured by the adequacy of the security. If that is not the case, then you may be able to use a “migration” to RACF as an opportunity to re-implement security for DB2 in a way that better addresses the current security needs than what is currently in place.

If, on the other hand, the security currently in place does reasonably well match the current security needs of the organization, then converting the existing DB2 authorization table content is likely to be significantly less effort than re-implementing security for DB2 in RACF and will preserve the current security controls.

In this case the IBM provided RACFDB2 conversion tool is likely to be of help in that process, but before you begin it will be necessary to understand the options provided within the RACF implementation of DB2 security to convert the DB2 authorization table content to RACF commands that are consistent with the options you;ve chosen.



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

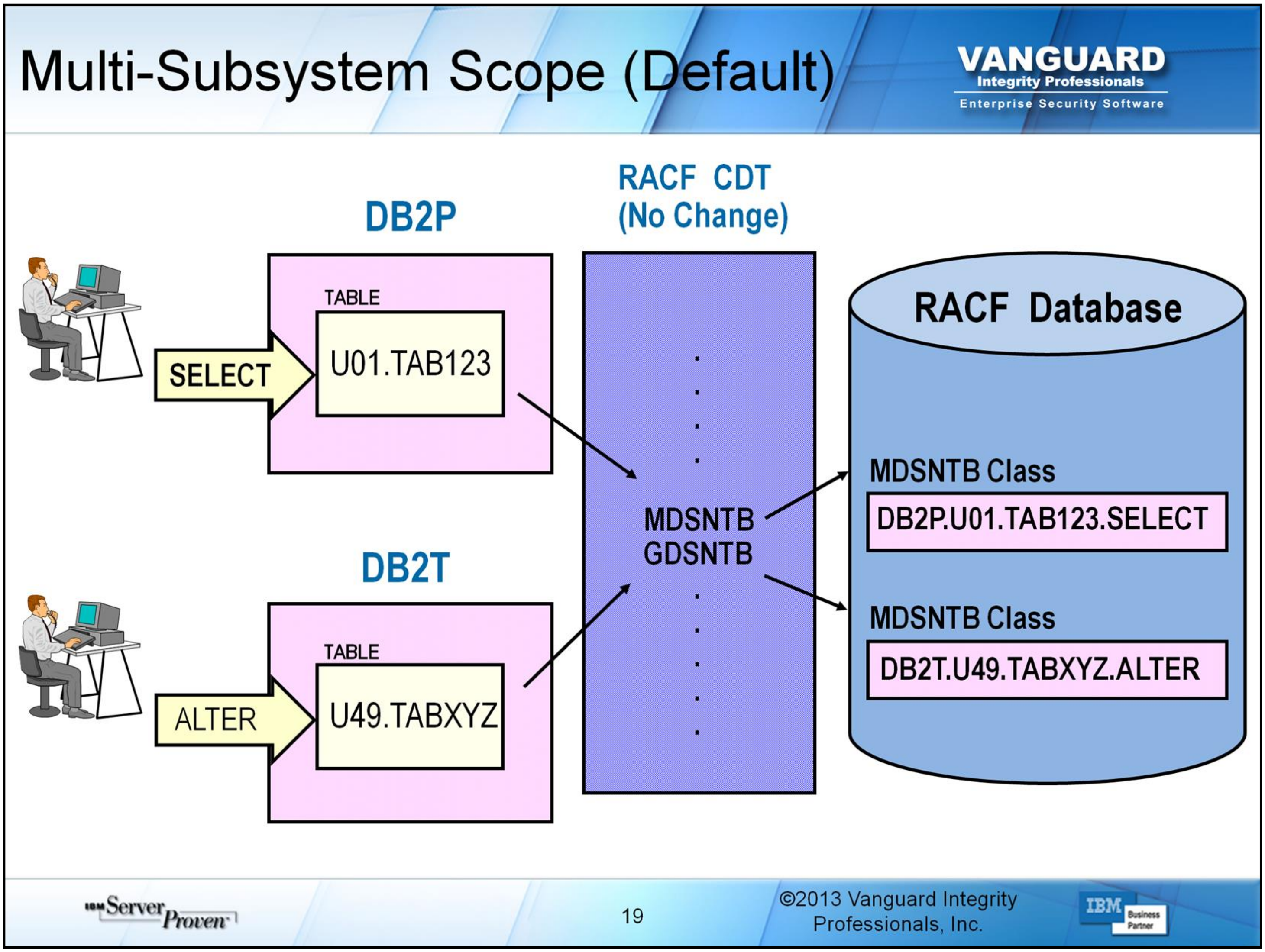
- Single Subsystem Scope Classes - Optional
  - DB2 subsystem name not in profile
  - DB2 subsystem name is part of the class name
  - Requires definitions to be added to CDT class
  - Delegation of administrative authority by DB2 sybsystem requires only CLAUTH

There are two different options in which the DB2 general resource classes can be implemented.

The default is “multi-subsystem scope” which means that one set of general resource classes is used for all the DB2 subsystems.

With multi-subsystem scope, all of the profiles for a type of DB2 object will be in the same general resource class pair with the individual profiles for each DB2 subsystem identified by the subsystem name as the high level qualifier for every profile.

Optionally, the installation can choose to define a set of general resource classes for each DB2 subsystem. This is known as “single subsystem scope”, in which each DB2 subsystem has its own set of general resource classes.



Multi-Subsystem Scope (Default)

VANGUARD Integrity Professionals
Enterprise Security Software

DB2P

TABLE

SELECT

U01.TAB123

RACF CDT
(No Change)

MDSNTB
GDSNTB

RACF Database

MDSNTB Class

DB2P.U01.TAB123.SELECT

DB2T

TABLE

ALTER

U49.TABXYZ

MDSNTB Class

DB2T.U49.TABXYZ.ALTER

IBM ServerProven

IBM Business Partner

With multi-subsystem scope, the default general resource classes are used for all DB2 subsystems.

The first qualifier of the profile

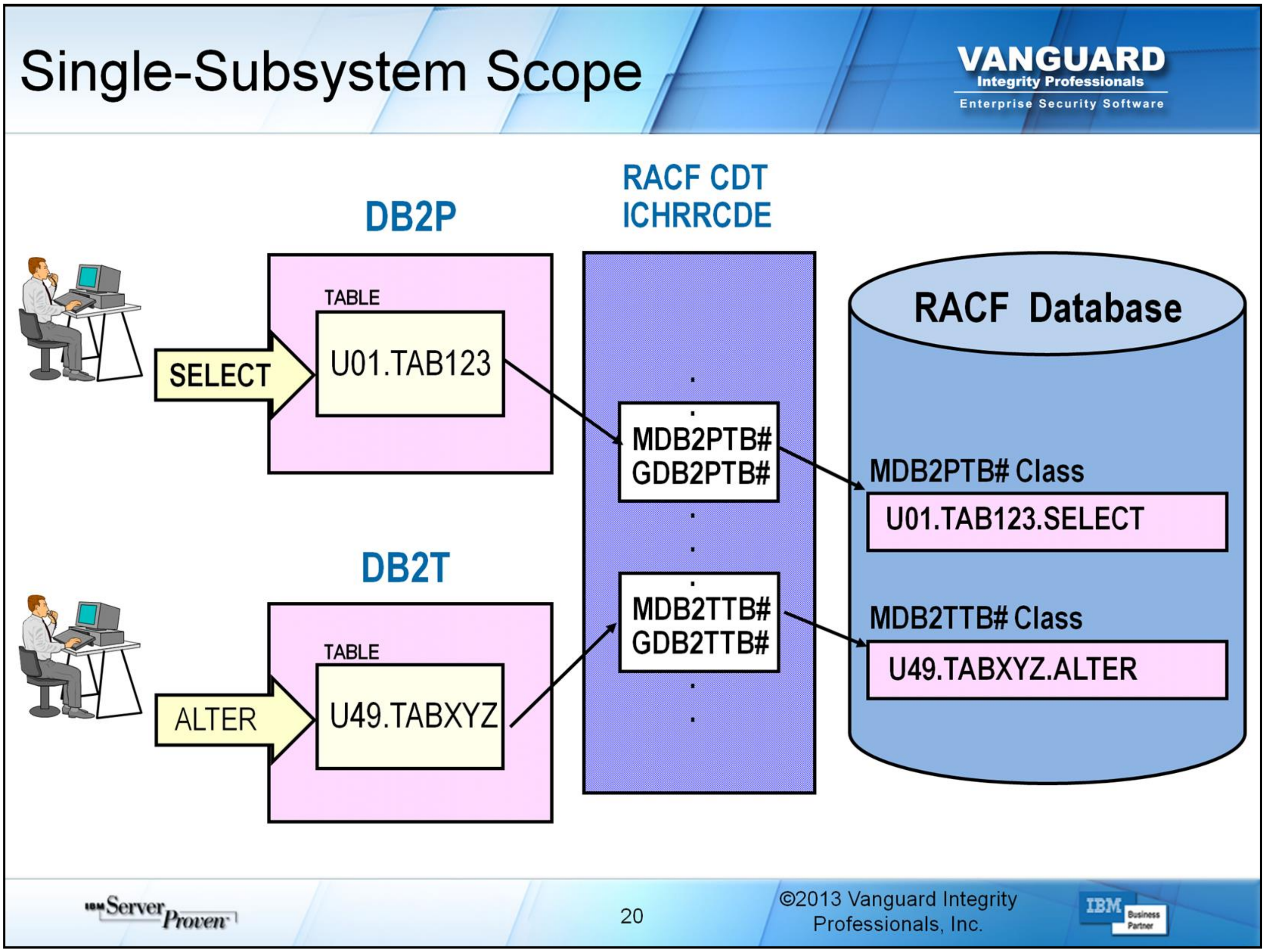
Is the DB2 subsystem name, or

Is the DB2 group attachment name when DB2 data sharing is used

The organization does not have to define any installation-defined general resource classes.

If the DB2 subsystem name changes, then the profiles must be deleted and created again.

Delegation of administrative authority for individual DB2 subsystems to users who do not have system SPECIAL authority can be accomplished with class authority (CLAUTH) and GENERICOWNER.



Single-Subsystem Scope

VANGUARD Integrity Professionals
Enterprise Security Software

DB2P

TABLE

SELECT

U01.TAB123

RACF CDT
ICHRRCDE

MDB2PTB#
GDB2PTB#

MDB2TTB#
GDB2TTB#

RACF Database

MDB2PTB# Class

U01.TAB123.SELECT

MDB2TTB# Class

U49.TABXYZ.ALTER

DB2T

TABLE

ALTER

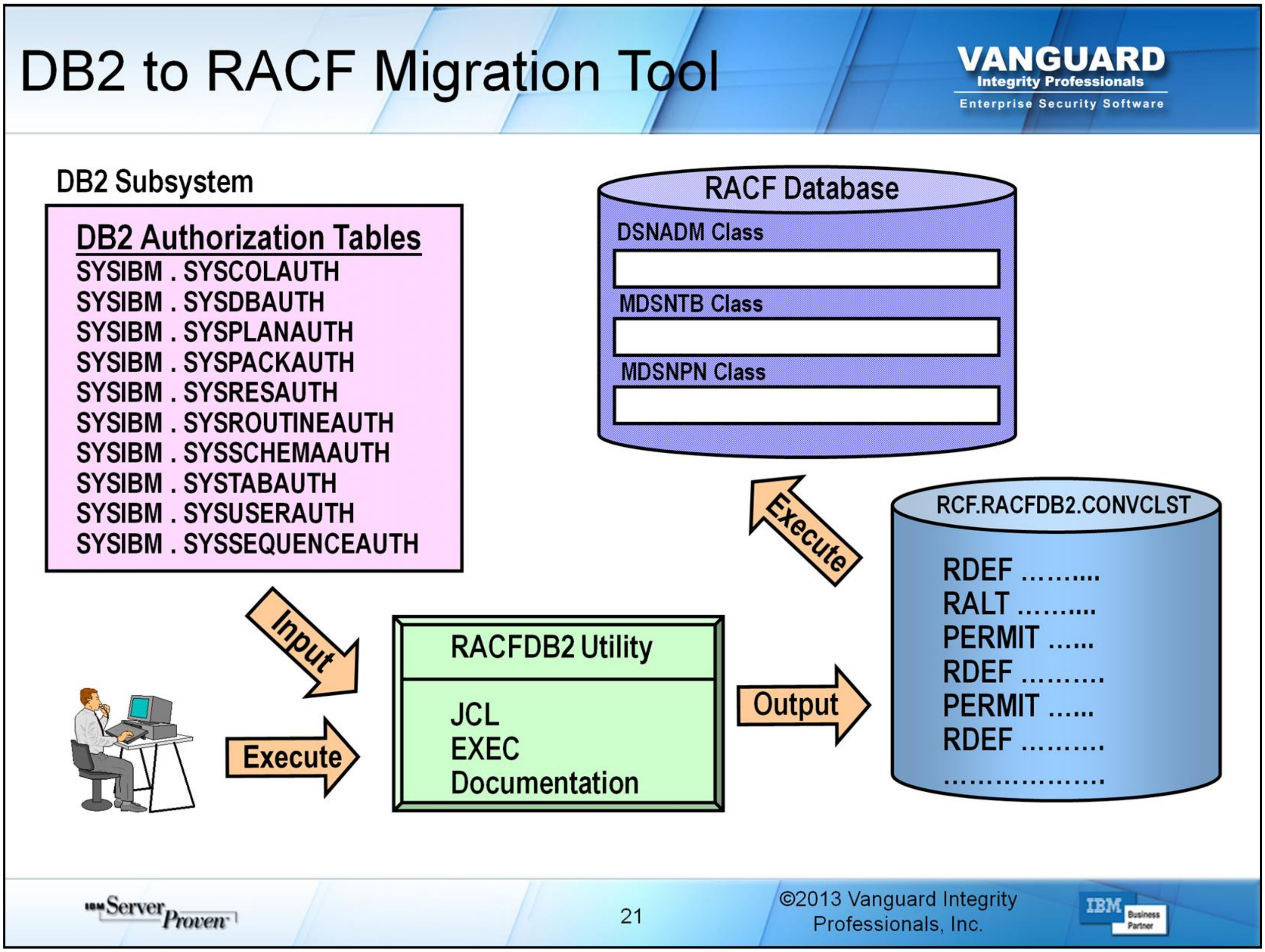
U49.TABXYZ

For single subsystem scope the organization must define general resource classes in the CDT (class descriptor table) general resource class before profiles for individual DB2 subsystems can be defined.

A set of DB2 general resource classes need to be defined for each DB2 subsystem.

Note that the DB2 subsystem name is not the included in the profile name, as with profiles used for multi-subsystem scope, as the subsystem name becomes part of the resource class name for each subsystem.

Delegation of administrative authority for individual DB2 subsystems to users who do not have system SPECIAL authority can be accomplished by using class authority (CLAUTH).



DB2 to RACF Migration Tool

VANGUARD
Integrity Professionals
Enterprise Security Software

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

RCF.RACFDB2.CONVCLST

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

Execute

There are three versions of the DB2 to RACF Migration Tool.

RACFDB2/RXSQL which requires the RXSQL product (5764-074)

RACFDB2/BatchPipes which requires the BatchPipes or MVS Pipes product

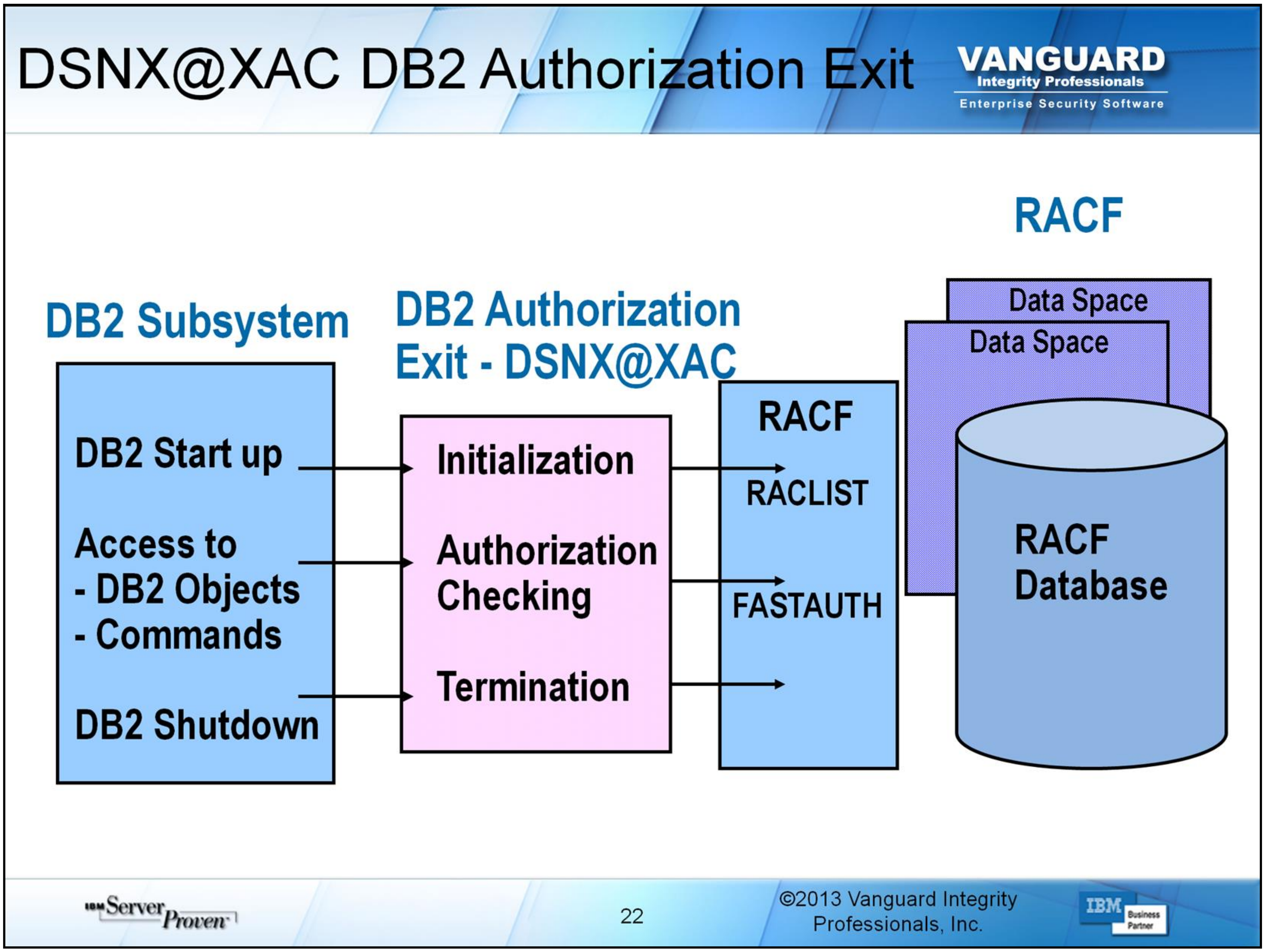
RACFDB2 for V6 and all later versions of DB2.

Each utility is made up of a set of JCL, an EXEC, and documentation.

The SYSIBM.SYSxxxxAUTH tables are input to each of the three utility versions.

The utility generates RACF commands and writes them to a CLIST data set.

The TSO Terminal Monitor Program (IKJEFT01) can be used to execute the generated RACF commands.



DSNX@XAC DB2 Authorization Exit

RACF

DB2 Subsystem

DB2 Start up

Access to
- DB2 Objects
- Commands

DB2 Shutdown

DB2 Authorization Exit - DSNX@XAC

Initialization

Authorization Checking

Termination

RACF

RACLIST

FASTAUTH

Data Space

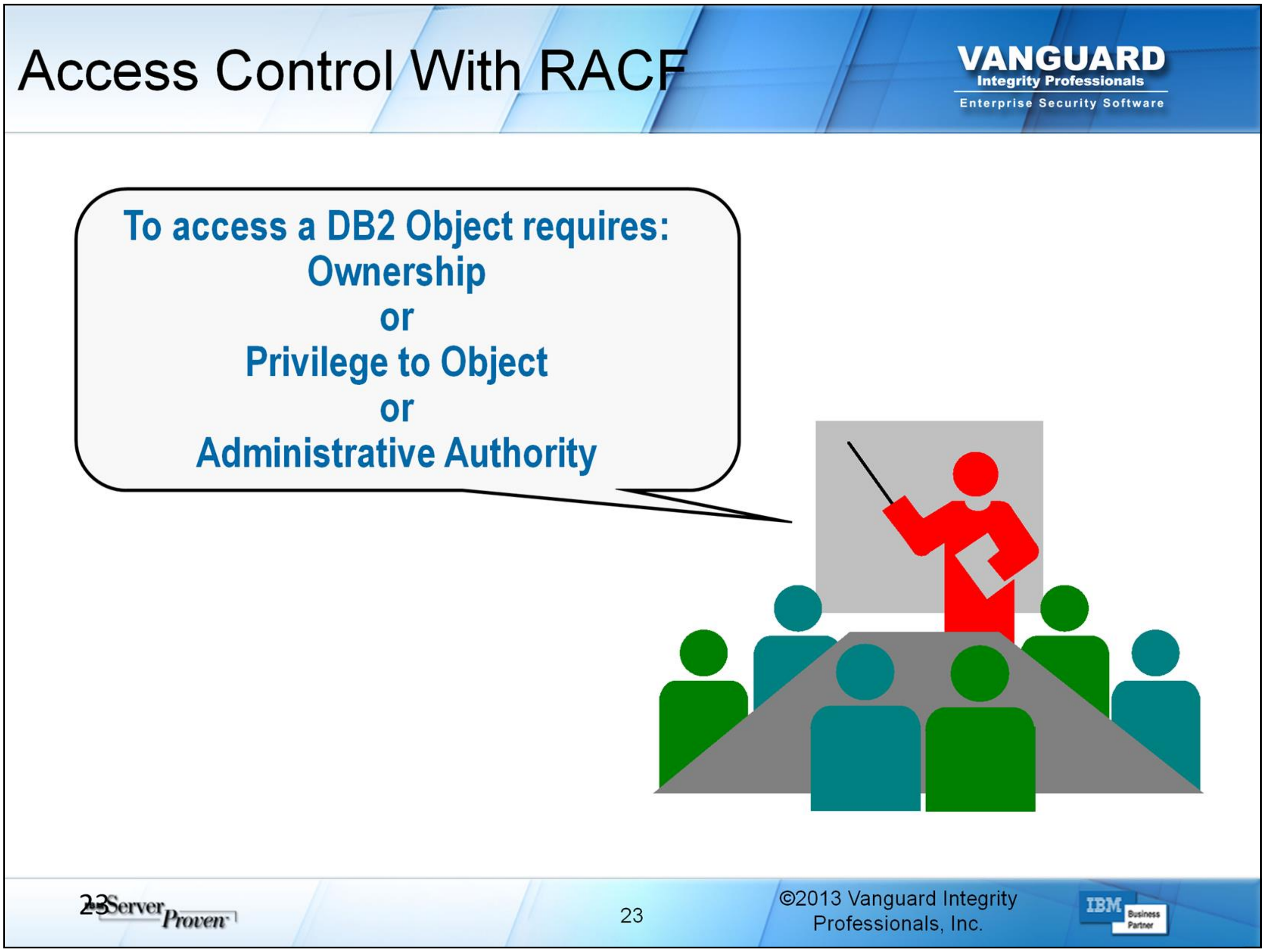
Data Space

RACF Database

The RACF/DB2 External Security Module (DSNX@XAC) provides the functions for RACF authorization.

The DB2 authorization Exit provides the following functions:

- Initialization - Loads profiles for RACF/DB2 authorization checking into data spaces. The RACF classes targeted for use must be active.
- Authorization Checking - Checks the user's authority to specified DB2 resources.
- Termination - Cleans up the connection to the profiles loaded in data spaces.



Access Control With RACF

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

Depending on the type of DB2 object, a user can access the object by having:

Ownership of the object

Privilege to the object

Administrative authority

For example, to SELECT from a table, the user must have either:

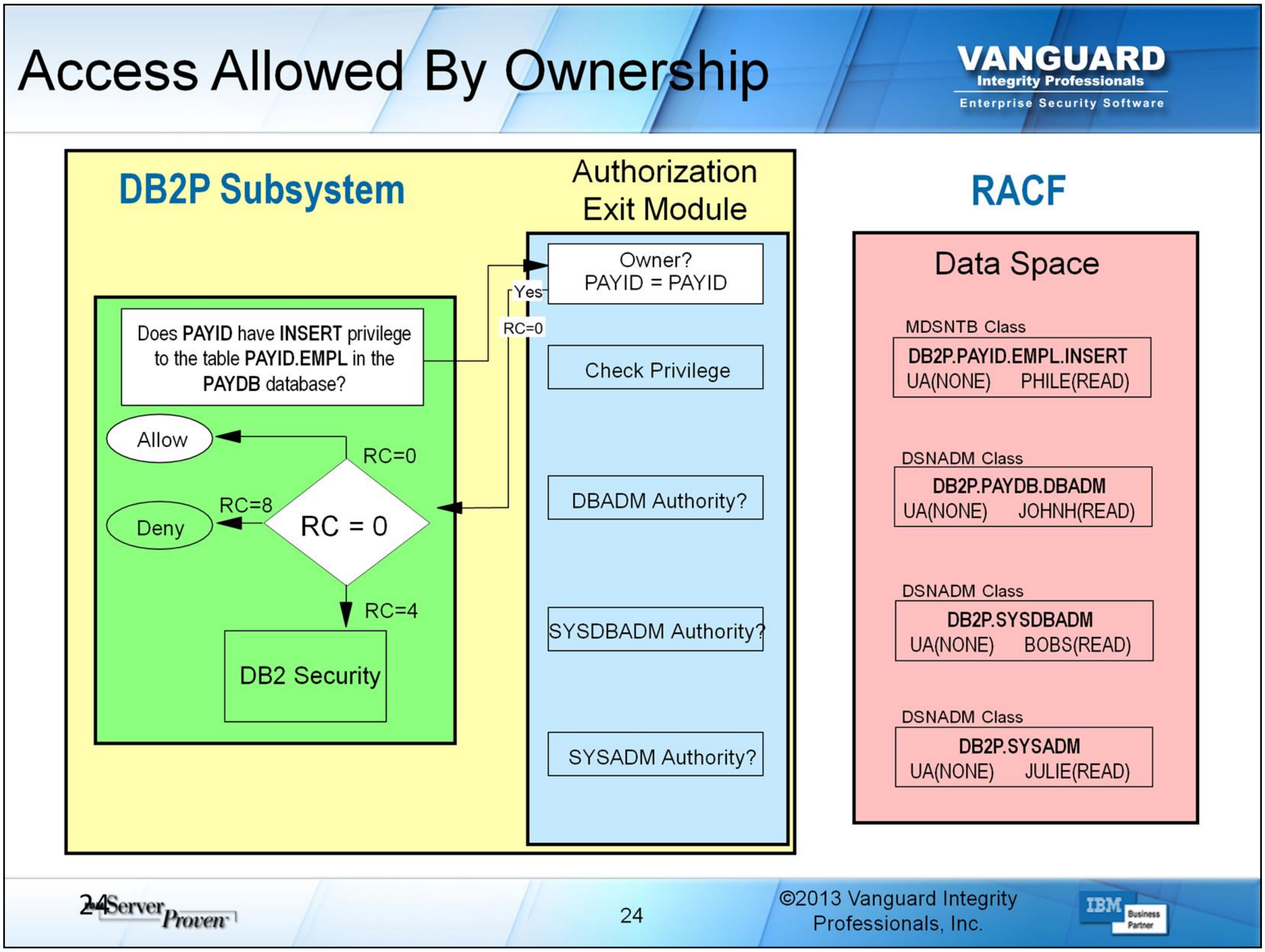
Ownership of the table

SELECT privilege to the table

DBADM authority for the database

SYSDBADM authority for the database

SYSADM administrative authority



Access Allowed By Ownership

VANGUARD Integrity Professionals

Enterprise Security Software

DB2P Subsystem

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

Allow

Deny

RC=0

RC=8

RC = 0

RC=4

DB2 Security

Authorization Exit Module

Yes

RC=0

Owner? PAYID = PAYID

Check Privilege

DBADM Authority?

SYSDBADM Authority?

SYSADM Authority?

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)

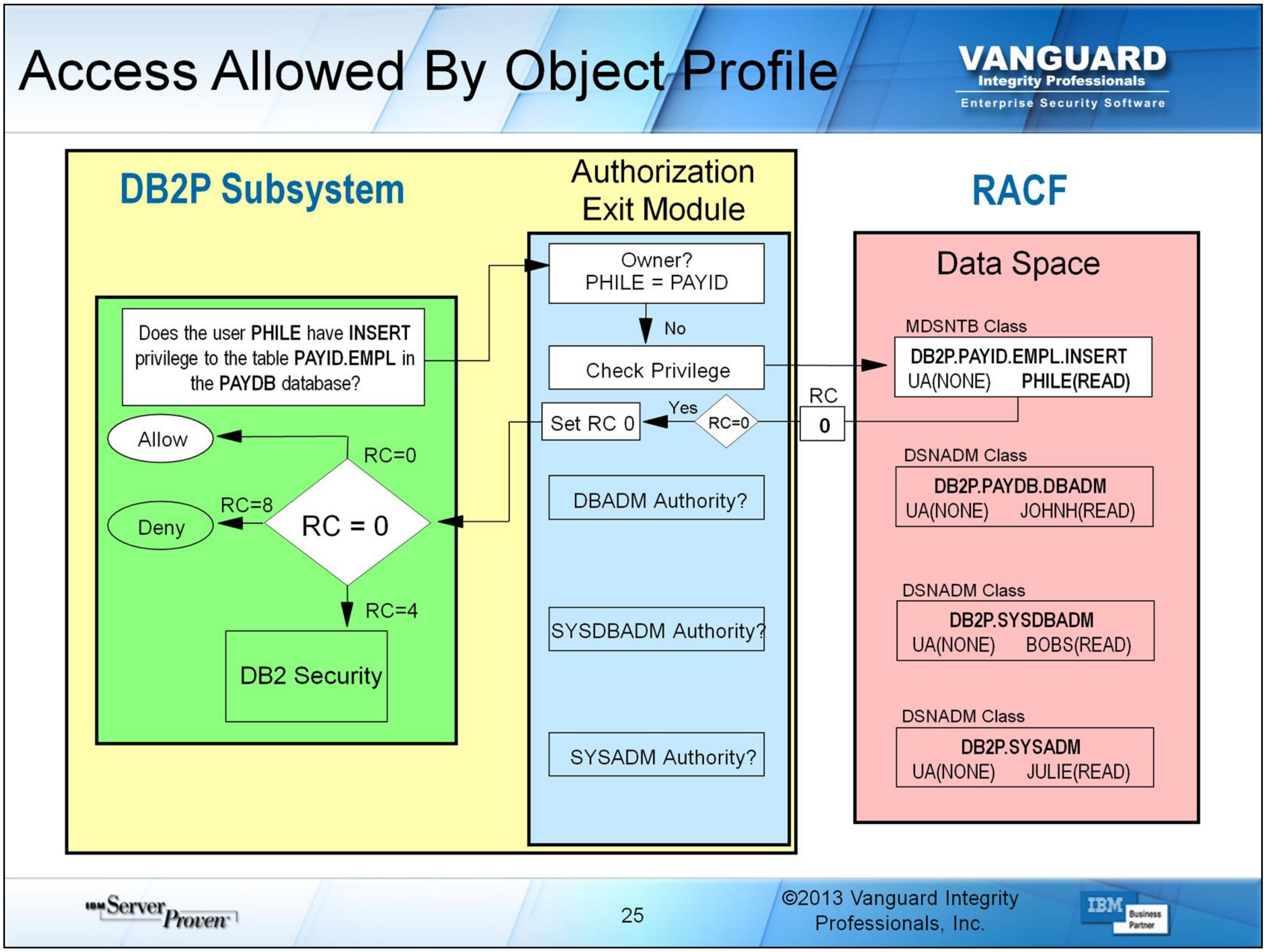
In this example, the PAYID user wants to INSERT a row in the table PAYID.EMPL.

DB2 calls the DSNX@XAC authorization exit.

Since PAYID is the owner of the table, the exit returns to DB2 with RC=0.

DB2 then allows access.

Note that RACF is not called.



Access Allowed By Object Profile

VANGUARD
Integrity Professionals
Enterprise Security Software

DB2P Subsystem

Authorization Exit Module

RACF

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

Owner?
PHILE = PAYID

No

Check Privilege

Yes

RC=0

Set RC 0

RC

0

Allow

RC=0

RC=8

Deny

RC = 0

RC=4

DB2 Security

DBADM Authority?

SYSDBADM Authority?

SYSADM Authority?

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)

In this example, user PHILE wants to insert a row into the PAYID.EMPL table.

DB2 calls the authorization exit

PHILE is not the owner of the table

The exit calls RACF with RACROUTE FASTAUTH in the MDSNTB class

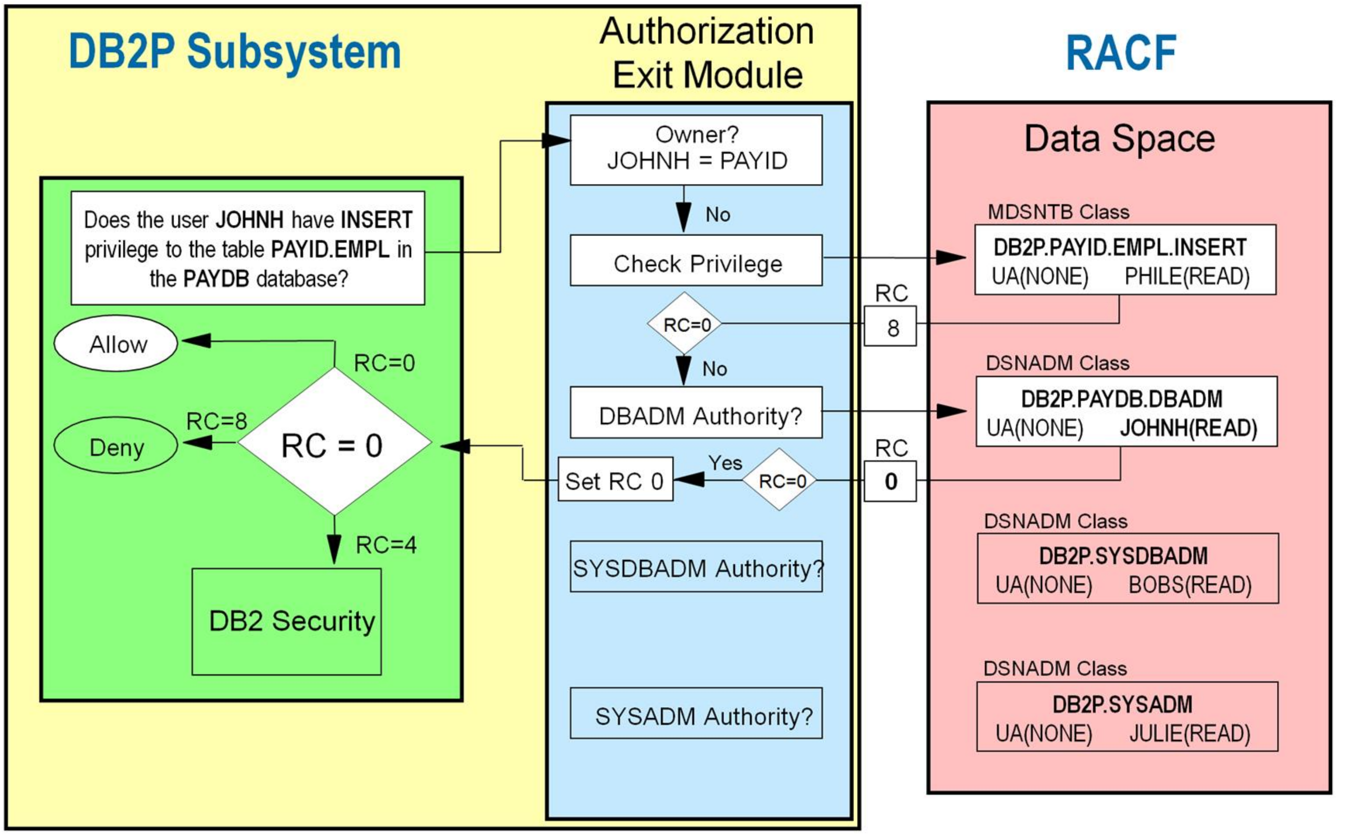
Since PHILE has read access, RACF returns with a RC=0.

The exit then sets the return code to RC=0 and returns to DB2

DB2 then allows the access

Note that RACF is called only one time.

Access Allowed By Admin Authority



DB2P Subsystem

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

Allow

Deny

RC=0

RC=8

RC = 0

RC=4

DB2 Security

Authorization Exit Module

Owner?
JOHNH = PAYID

No

Check Privilege

RC=0

No

DBADM Authority?

Yes

Set RC 0

RC=0

SYSDBADM Authority?

SYSADM Authority?

RC
8

RC
0

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)

In this example, JOHNH wants to insert a row in the PAYID.EMPL table.

DB2 calls the DSNX@XAC exit

JOHNH is not the owner of the table

The exit calls RACF to find out if JOHNH has INSERT privilege.

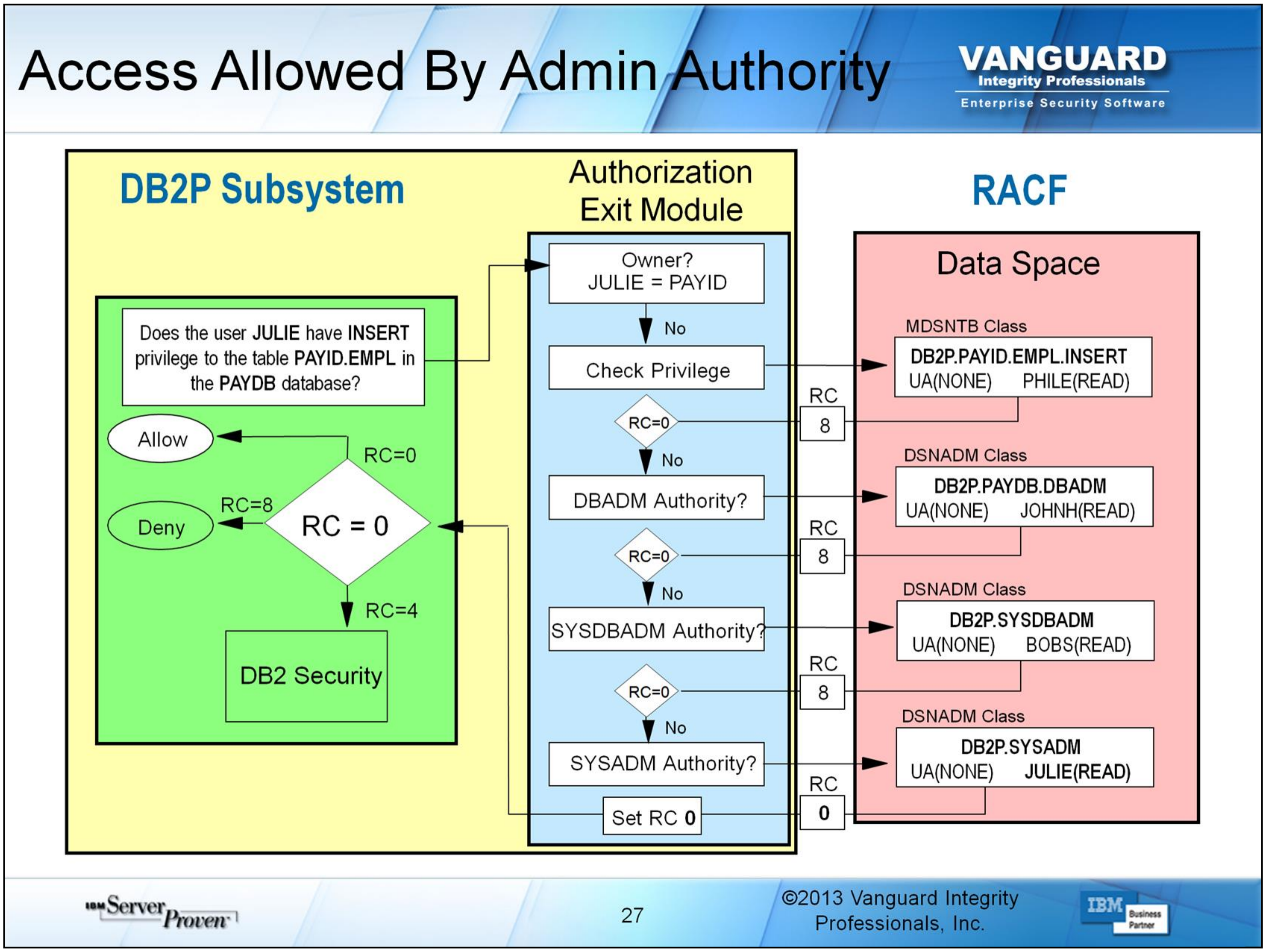
RACF returns a RC=8 because JOHN does not have INSERT privilege

Next, the exit calls RACF to find out if JOHNH has DBADM authority for the PAYDB database.

RACF returns a RC=0 because JOHNH does have DBADM authority

The authorization exit then sets the RC=0 and returns to DB2.

DB2 allows the access.



Access Allowed By Admin Authority

In this example, user JULIE wants to insert a row in table PAYID.EMPL.

DB2 calls the authorization exit to check access

JULIE is not the owner

The exit calls RACF to find out if she has the INSERT privilege for the table.

RACF returns a RC=8 since JULIE does not have access

Next, the exit calls RACF to see if JULIE has DBADM authority for the PAYDB database.

RACF returns a RC=8 since JULIE does not have access

Next, the exit calls RACF to see if JULIE has SYSDBADM authority.

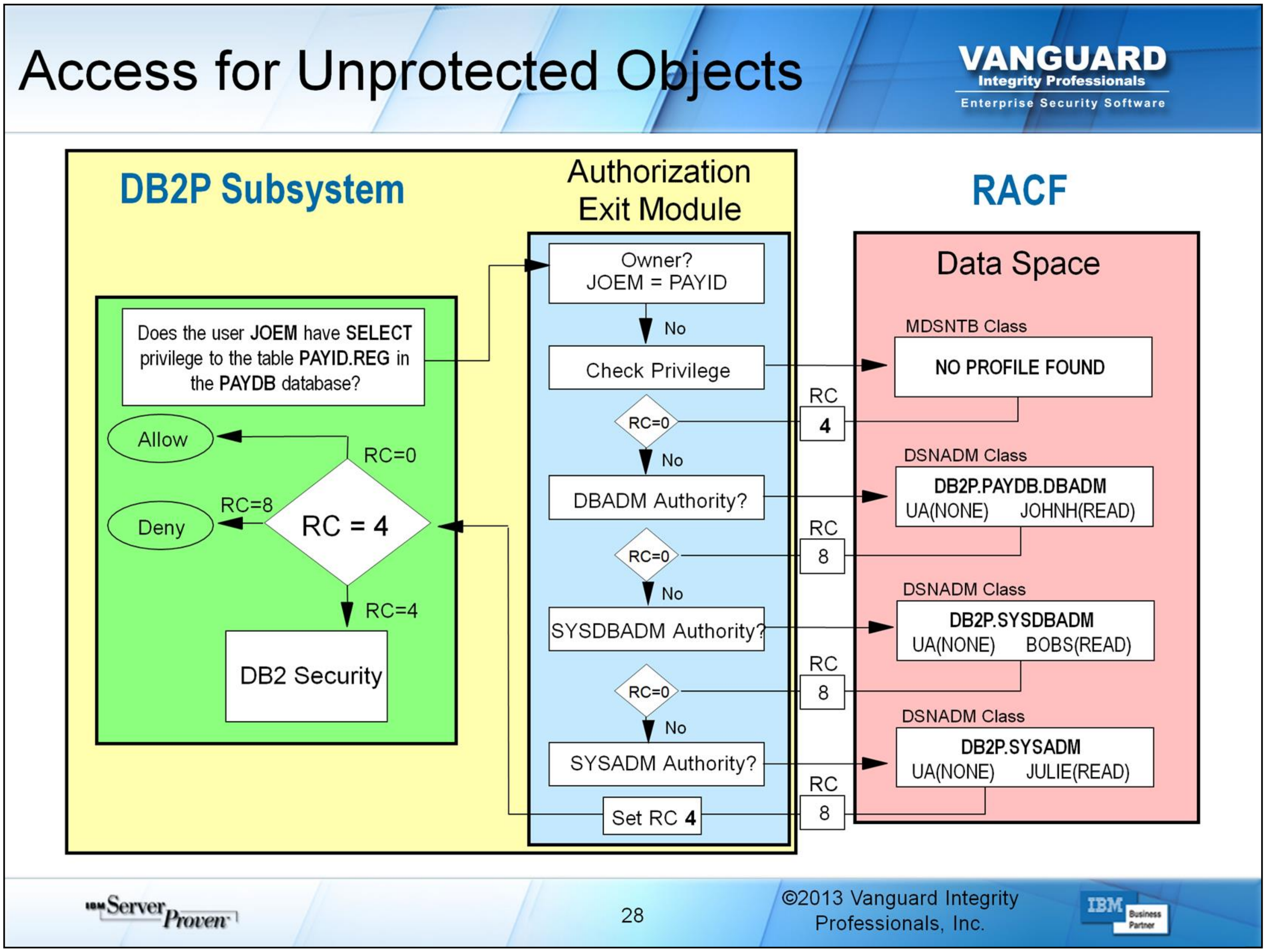
RACF returns a RC=8 since JULIE does not have access

The exit calls RACF to find out if she has SYSADM authority.

RACF returns a RC=0 since JULIE does have SYSADM authority

Finally, the exit sets the RC=0 and returns to DB2.

DB2 allows the access.



Access for Unprotected Objects

VANGUARD Integrity Professionals
Enterprise Security Software

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)

IBM Server Proven

IBM Business Partner

In this example, the user JOEM wants to select a row in table PAYID.REG.

DB2 calls the authorization exit

JOEM is not the owner of table PAYID.REG

The exit calls RACF to find out if JOEM has the SELECT privilege to the PAYID.REG table.

RACF returns with RC=4 because a profile does not exist

The exit next calls RACF to find out if JOEM has DBADM for the PAYDB database.

RACF returns with RC=8 because JOEM does not have DBADM

The exit next calls RACF to find out if JOEM has SYSDBADM authority.

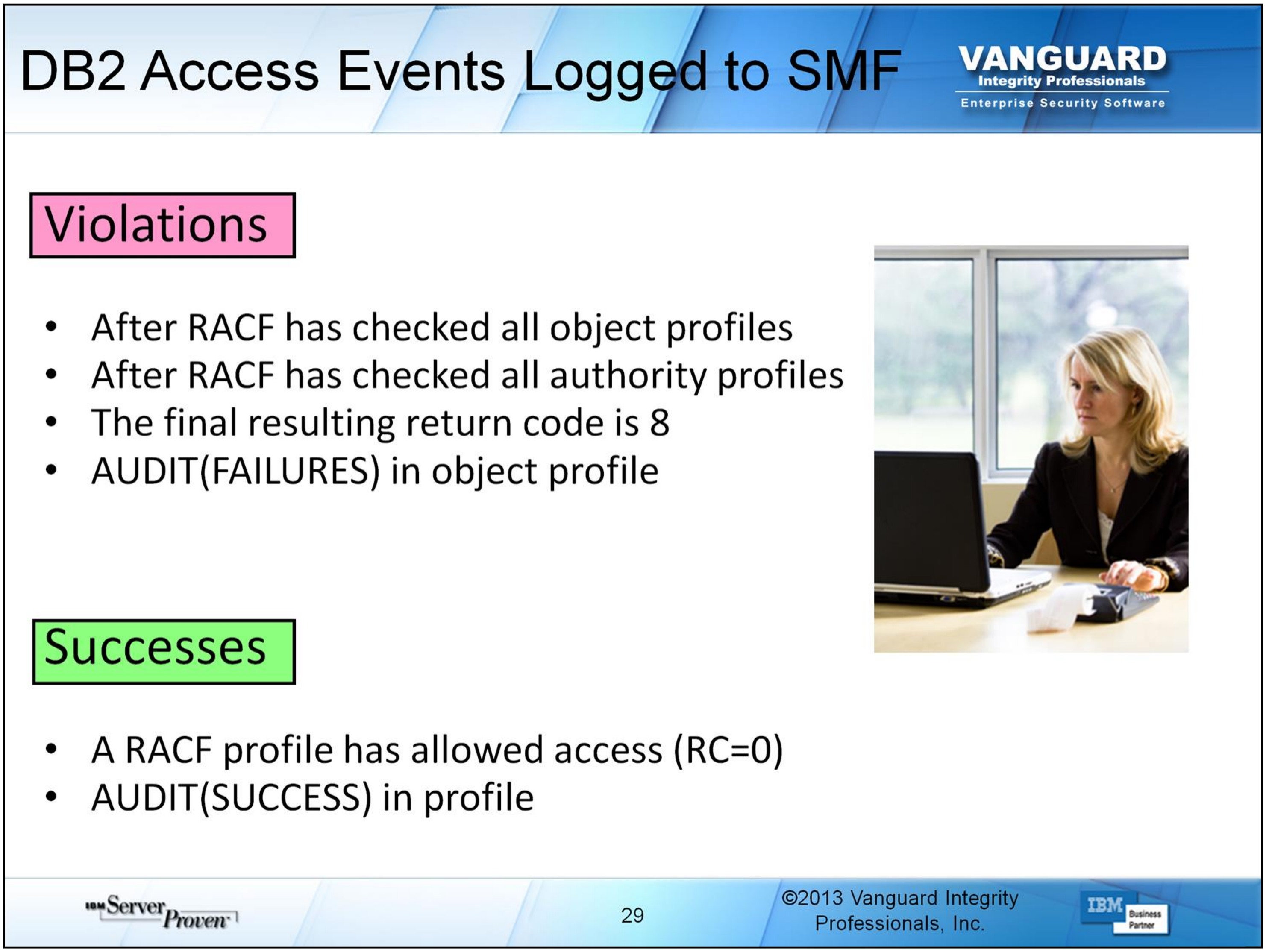
RACF returns with RC=8 because JOEM does not have SYSDBADM

The exit calls RACF to find out if JOEM has SYSADM authority.

RACF returns with a RC=8 because JOEM does not have SYSADM

The authorization exit now sets RC=4 to indicate to defer the decision to DB2.

Finally, DB2 looks at table SYSIBM.SYSTABAUTH to decide whether to allow or deny access.



DB2 Access Events Logged to SMF

VANGUARD
Integrity Professionals
Enterprise Security Software

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

IBM Server Proven
IBM Business Partner

The DSNX@XAC exit may call RACF zero or several times before making the final access decision.

If the access was allowed because of ownership, then RACF is not called and no SMF record can be written.

If the access decision is deferred to DB2, then RACF does not write an SMF record.

If the DSNX@XAC exit has decided to send a RC=8 back to DB2, then a violation is written.

If any object or authority profile allowed access (RC=0), then the success is logged if AUDIT(SUCCESS) is specified in the profile that allowed access.

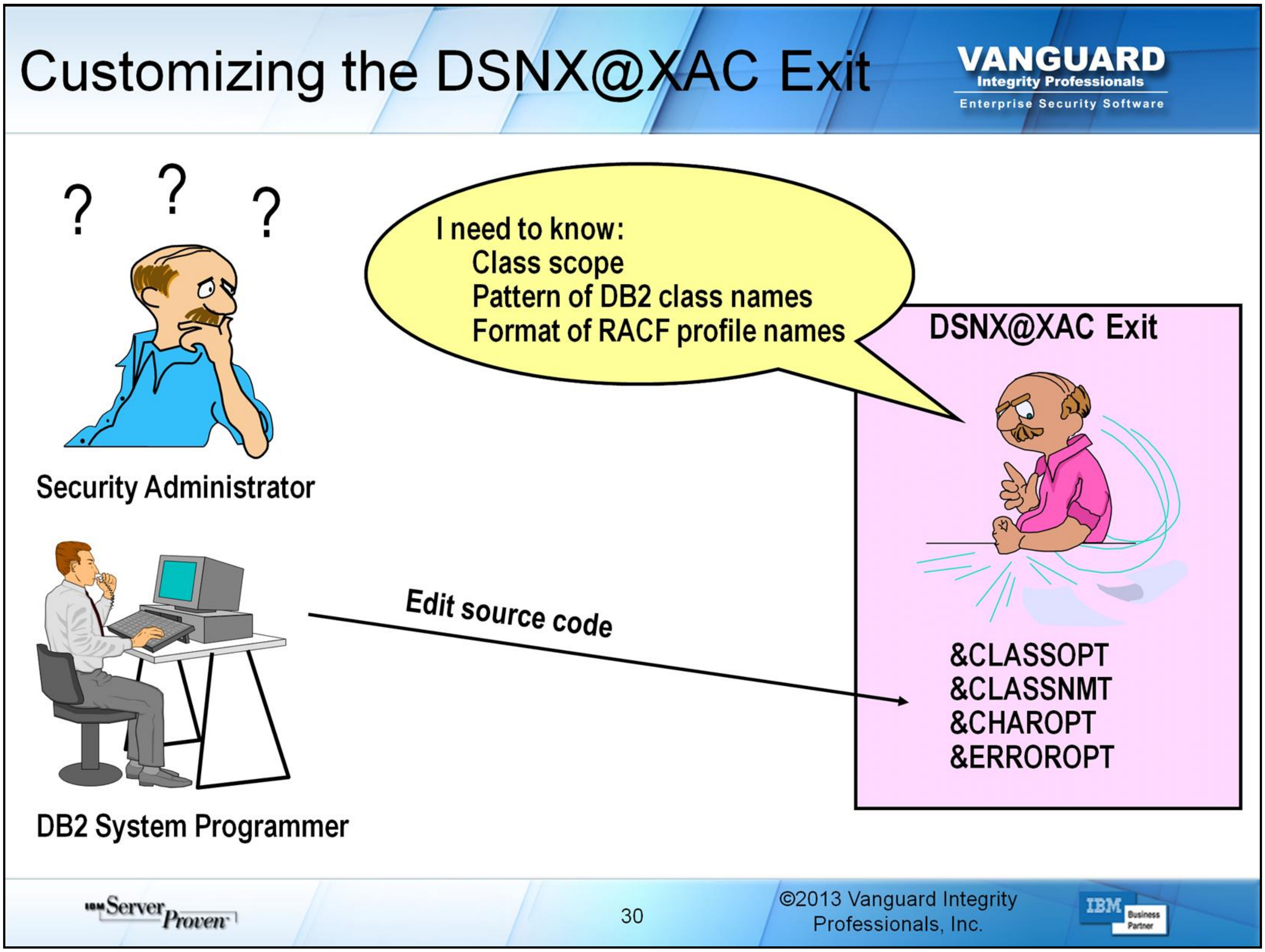
It is possible to get a “misleading” violation for table access if the user gets access via “columns” authority.

Access is checked first to see if the user has access to the entire table

If the user fails that check, an audit record might be written

Next, access is checked to see if the user has access to specific columns

If the access is allowed, then the SMF record written for the previous failure is misleading



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

&CLASSOPT
&CLASSNMT
&CHAROPT
&ERROROPT

Edit source code

DB2 System Programmer

Before installing the DSNX@XAC access control authorization exit, you need to make some decisions, or you could just take the defaults and not worry!

You specify the class scope (also known as the classification model) in &CLASSOPT

You specify the class name root in &CLASSNMT

You specify the last character of the classname in &CHAROPT

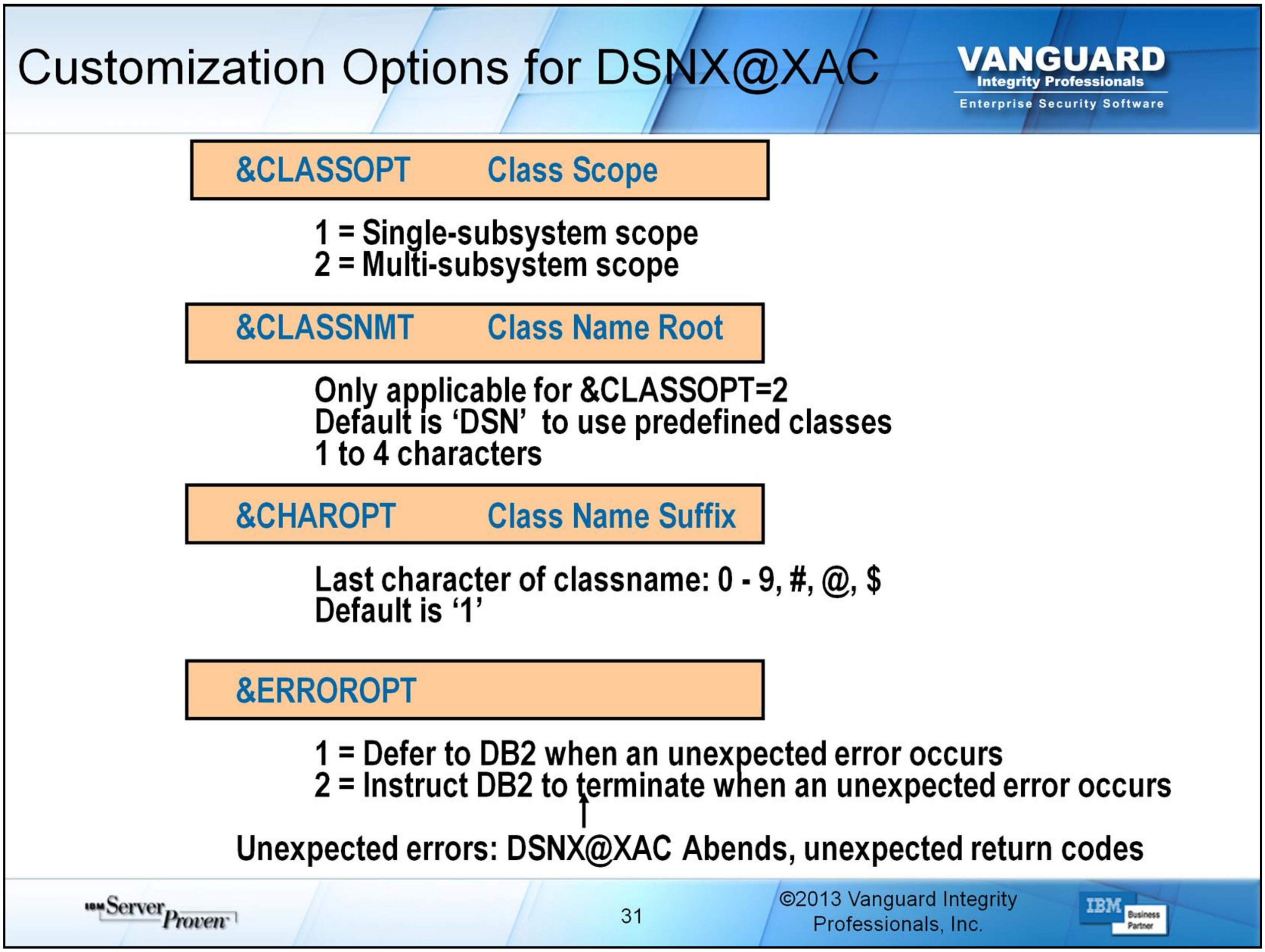
You specify what action to take when an unexpected error occurs in &ERROROPT

In addition, there are two other settings that the exit needs:

&PCELLCT - number of primary work area cells (default is 50)

&SCELLCT - number of secondary work area cells (default is 50)

The system programmer edits the DSNX@XAC source code to replace the default values.



Customization Options for DSNX@XAC

VANGUARD Integrity Professionals
Enterprise Security Software

&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

You specify the class scope (classification model) in &CLASSOPT:

‘1’ is Single-Subsystem Scope, which means one set of resource profiles for each DB2 subsystem

‘2’ is Multi-Subsystem Scope, which means one set of resource profiles for all DB2 subsystems The default is ‘2’

You specify the class name root in &CLASSNMT:

Applies only for &CLASSOPT=2

1 to 4 characters in positions 2 through 5 of classname

The default is ‘DSN’

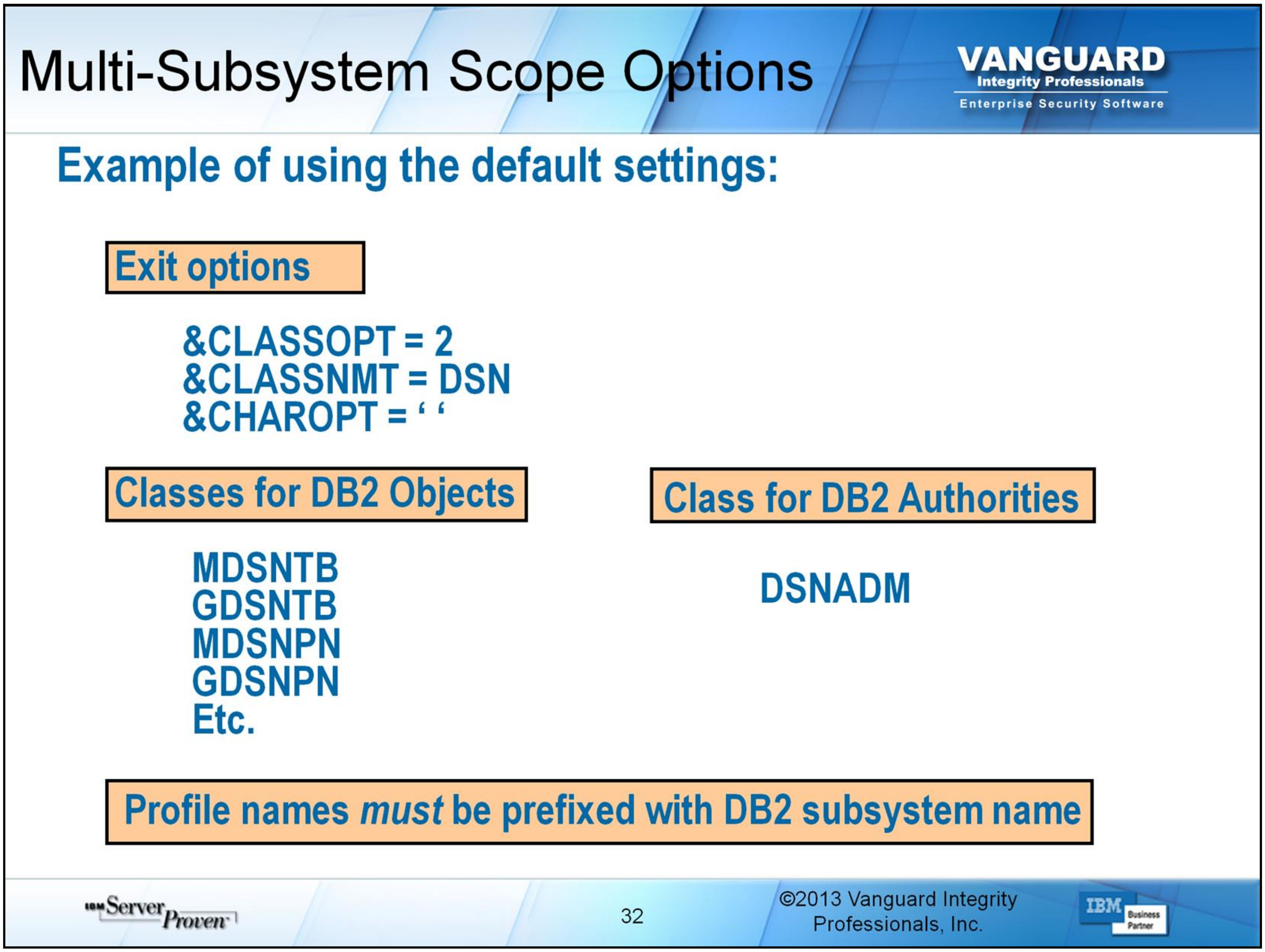
You specify the class name suffix in &CHAROPT:

Last character of the classname

Valid characters are 0 through 9, #, @, or $

The default is ‘1’

In addition to &ERROROPT, there are two additional parameters that can be customized, &PCELLCT and &SCELLCT. &PCELLCT and &SCELLCT are the number of cells used as work areas. The default is 50 for each.



Multi-Subsystem Scope Options

Example of using the default settings:

Exit options

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

Classes for DB2 Objects

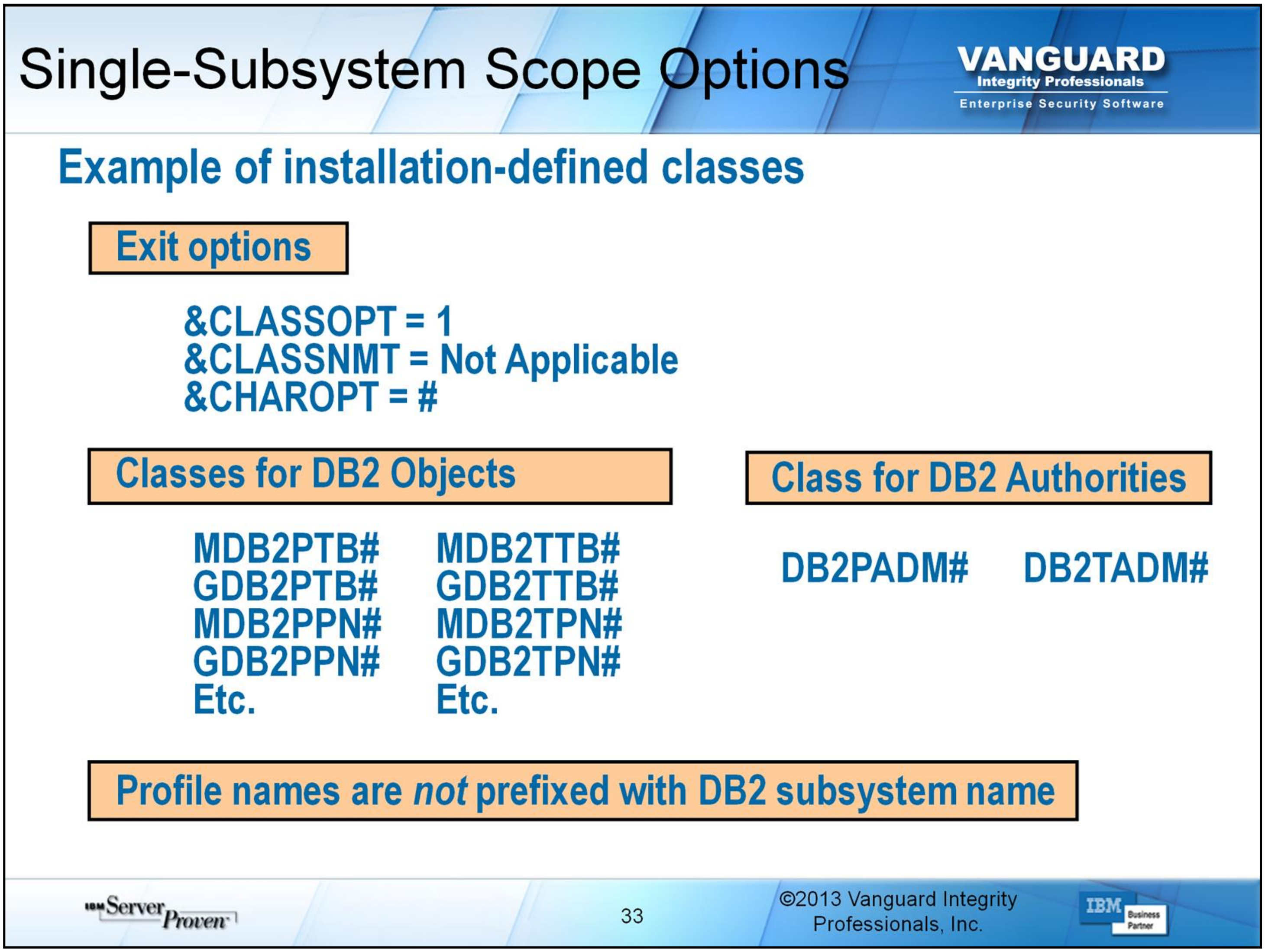
MDSNTB
GDSNTB
MDSNPN
GDSNPN
Etc.

Class for DB2 Authorities

DSNADM

Profile names *must* be prefixed with DB2 subsystem name

This example shows the conversion utility options for use with multi-subsystem scope and the corresponding RACF general resource class names used.



Single-Subsystem Scope Options

Example of installation-defined classes

Exit options

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

Classes for DB2 Objects

MDB2PTB#
GDB2PTB#
MDB2PPN#
GDB2PPN#
Etc.

MDB2TTB#
GDB2TTB#
MDB2TPN#
GDB2TPN#
Etc.

Class for DB2 Authorities

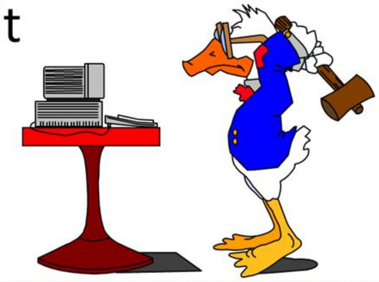
DB2PADM# DB2TADM#

Profile names are *not* prefixed with DB2 subsystem name

This example shows the conversion utility options for use with single subsystem scope and the corresponding RACF general resource class names used for a particular DB2 subsystem.

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



The system programmer performs steps 1,2,3,5, 6, and 7

The DSNX@XAC module is delivered to you:

For DB2 V8 and later, see member DSNXRXAC in DB2 SDSNSAMP library

The RACF administrator performs steps 4, if needed

Modify sample exit source code to customize sample exit (optional)

&CLASSOPT - Single or Multi-subsystem scope

&CLASSNMT - Class name root

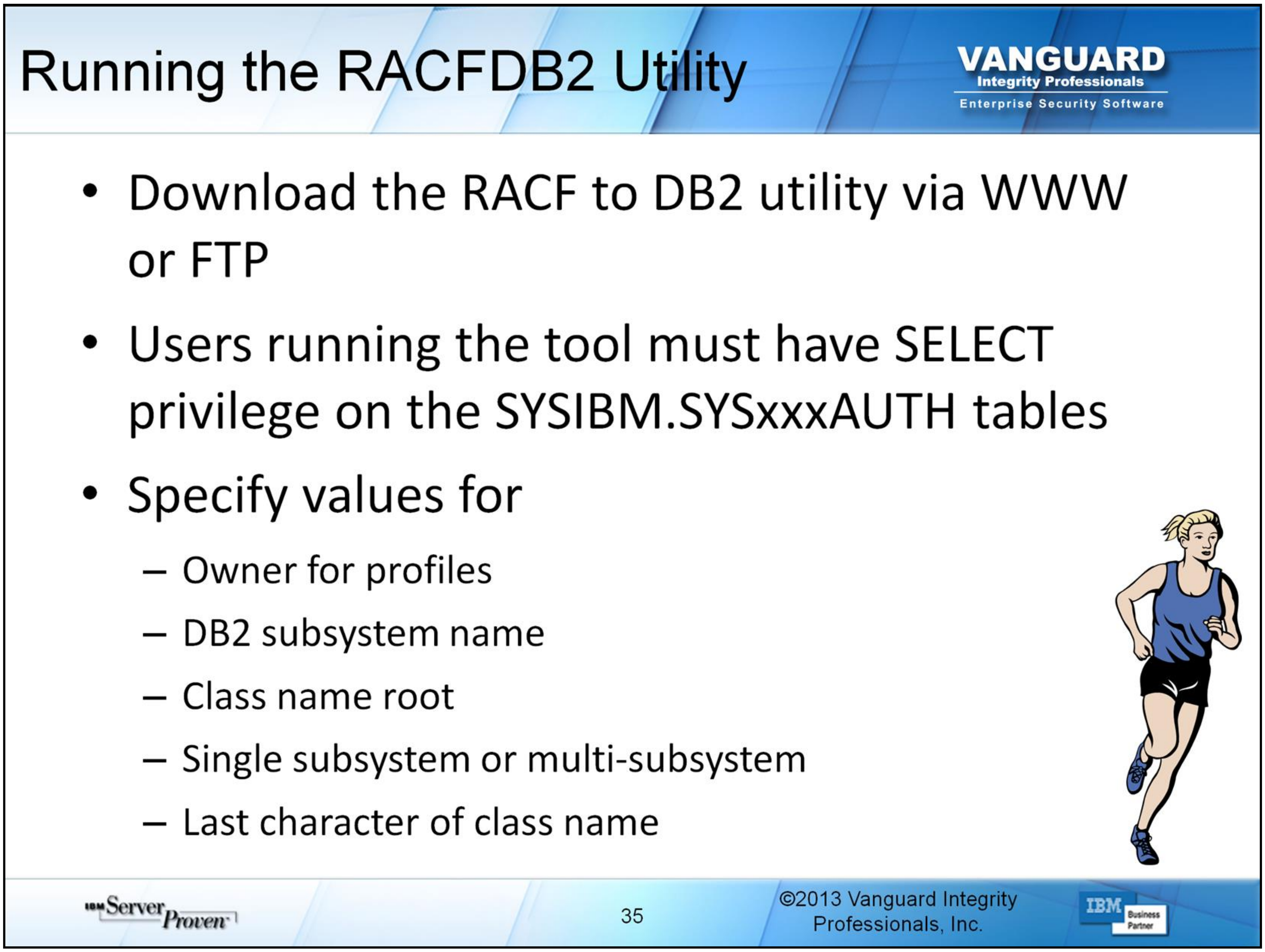
&CHAROPT - Last character of class name

&ERROROPT - Action to take when an unexpected error in the DSNX@XAC exit

It is not necessary to add installation-defined classes. The default classes can be used.

Modify the JEX0003 step of DSNTIJEX to point to library where DSNX@XAC is found.

After the exit is installed in the DB2 exit load library, RACF authorization checking will be done for any active classes.



Running the RACFDB2 Utility

- Download the RACF to DB2 utility via WWW or FTP
- Users 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

The tool is available from IBM via the Internet.

For WWW, point your browser to http://www.ibm.com/racf, then click on “Downloads”

For anonymous FTP, the site is s390.ibm.com

Each of the utilities consists of JCL, a REXX exec, and documentation.

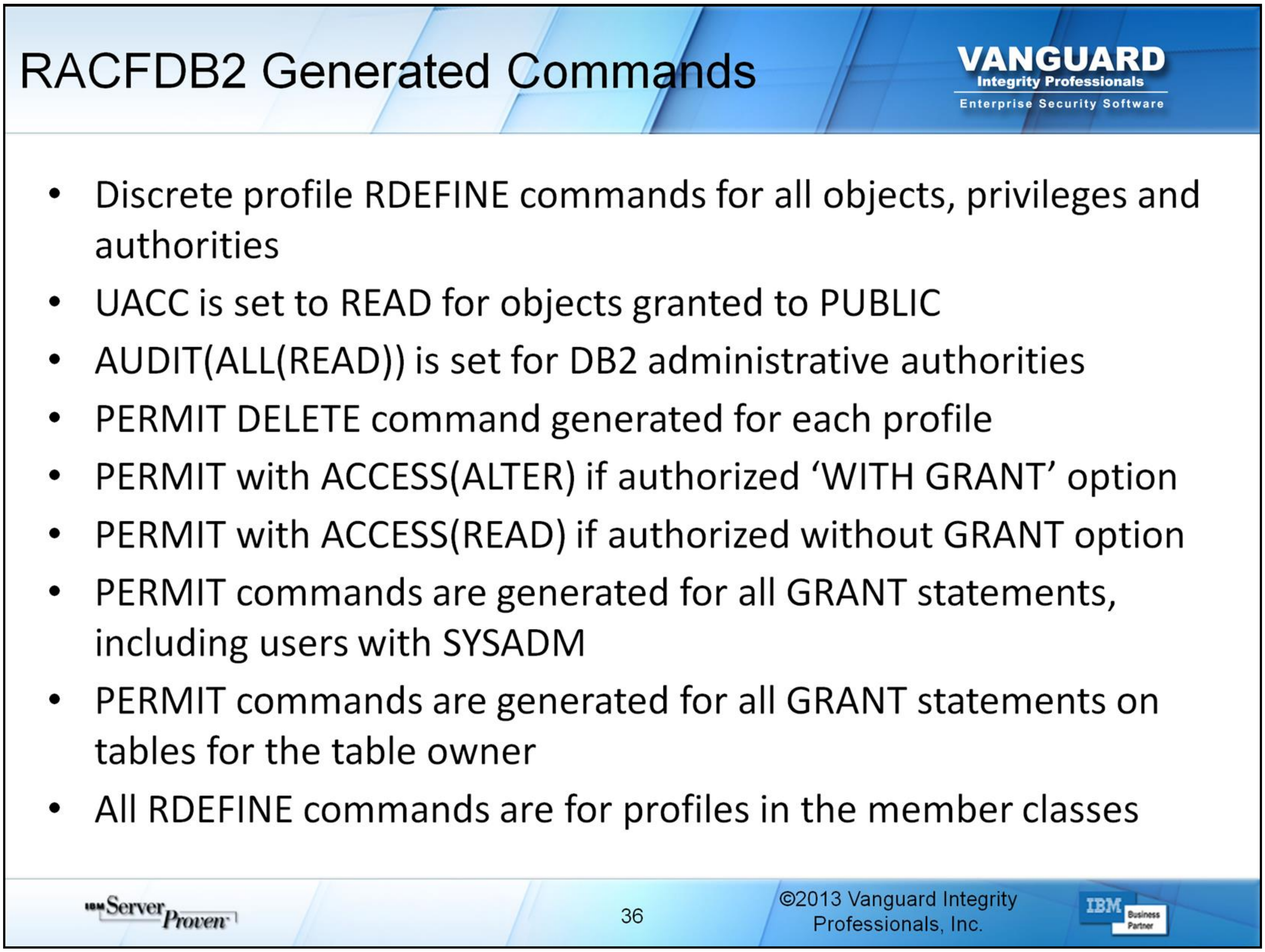
Another approach is described in the IBM redbook titled:

Ready for E-Business - OS/390 Security Server Enhancements, SG24-5158-00.

This lists the SQL statements that can be issued to produce RACF commands.

The commands produced are equivalent to commands produced by the RACF to DB2 migration utility.

However, the commands produced have to be edited to remove blanks before execution.



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

The DB2 to RACF Migration Utility scans the SYSIBM.SYSxxxAUTH tables.

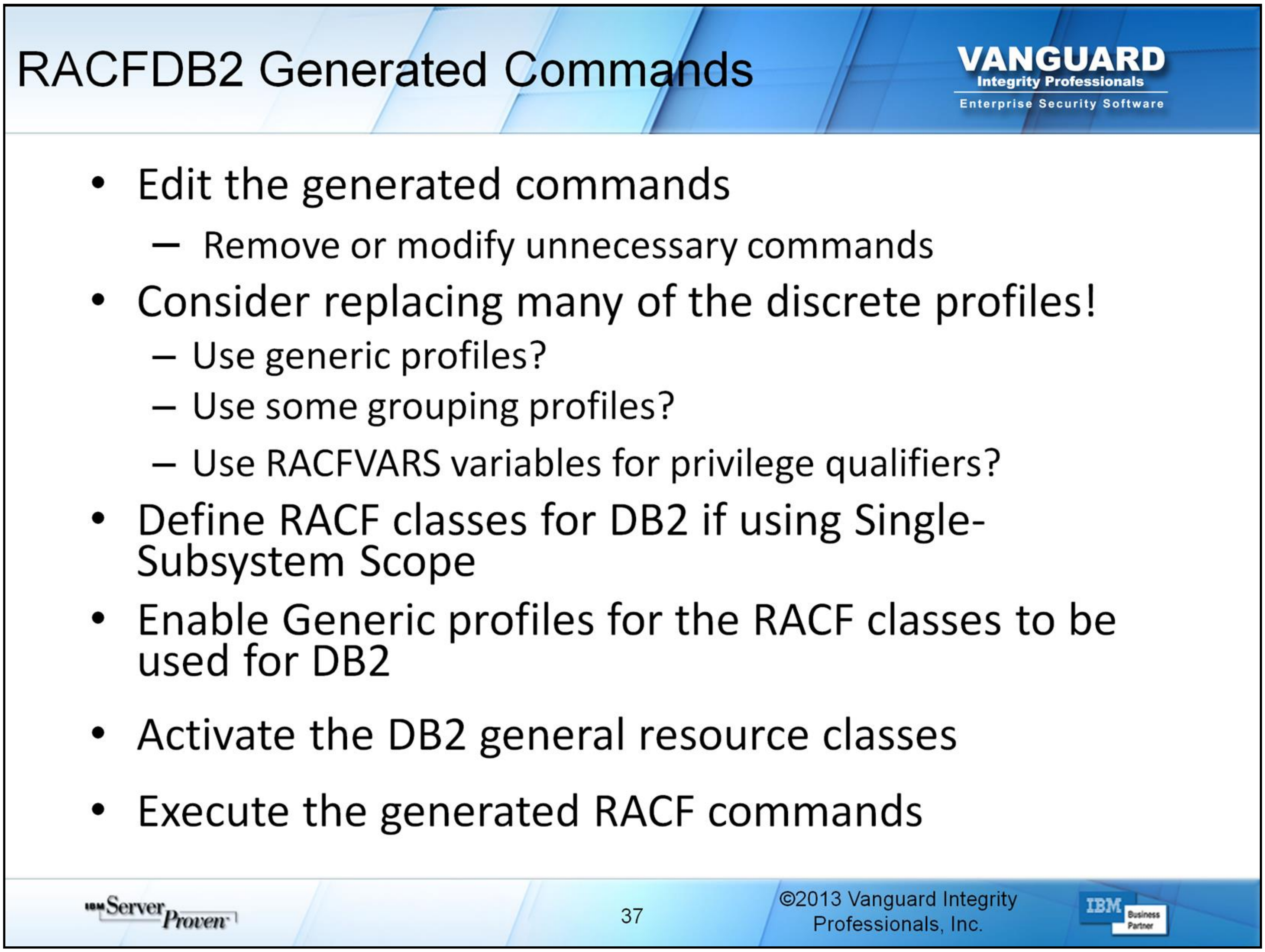
Note that the utility produces commands to create discrete profiles. You should consider replacing these with commands to create grouping profiles, generic profiles, and use RACFVARS variables to simplify security administration.

The utility generates RACF commands for each object/privilege/authority that must be protected.

For privileges granted to PUBLIC, the UACC is set to READ.

The migration utility does not check for PUBLIC that was GRANTed with the GRANT option.

In cases where an authorization id was GRANTed with GRANT, the utility builds a PERMIT command with an ACCESS of ALTER. This allows the user to PERMIT other users to this privilege since the profiles are discrete.



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

You absolutely will want to make many changes to the generated RACF commands.

Generic profiles will allow you to significantly reduce the number of profiles.

You may be able to simplify administration by combining some discrete profiles into grouping profiles.

Consider setting up a RACFVARS variable as appropriate. For example, if all three production DB2 environments have the same security, you could use a RACF variable for the subsystem-name qualifier of the profile name.

If the exit is activated, but the DB2 general resource classes are not active, the authorization exit will return a return code of 4 and the access decision will be deferred to DB2.

To execute the RACF commands generated by the RACFDB2 utility, the user must have either:

System-SPECIAL, or CLAUTH for the DB2 classes and group-SPECIAL over the profile owner

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
  - . . .

PUBLIC* (PUBLIC at all locations) is not supported directly. You could use a generic character in the ssn of profile.

There are some differences in implicit privileges of ownership for some objects.

In DB2 V 5 and V6, DB2 does not supply the database name for drop and alter index, and therefore RACF cannot check DBADM for the specific database. So, RACF checks for SYSCTRL, SYSADM, and the profile with a name of ssn.DBADM (class scope 2) or DBADM (class scope 1). DB2 V7 **does** supply the database name for drop and alter index, and therefore DBADM authority for the database is sufficient for the user to be able to drop or alter and index.

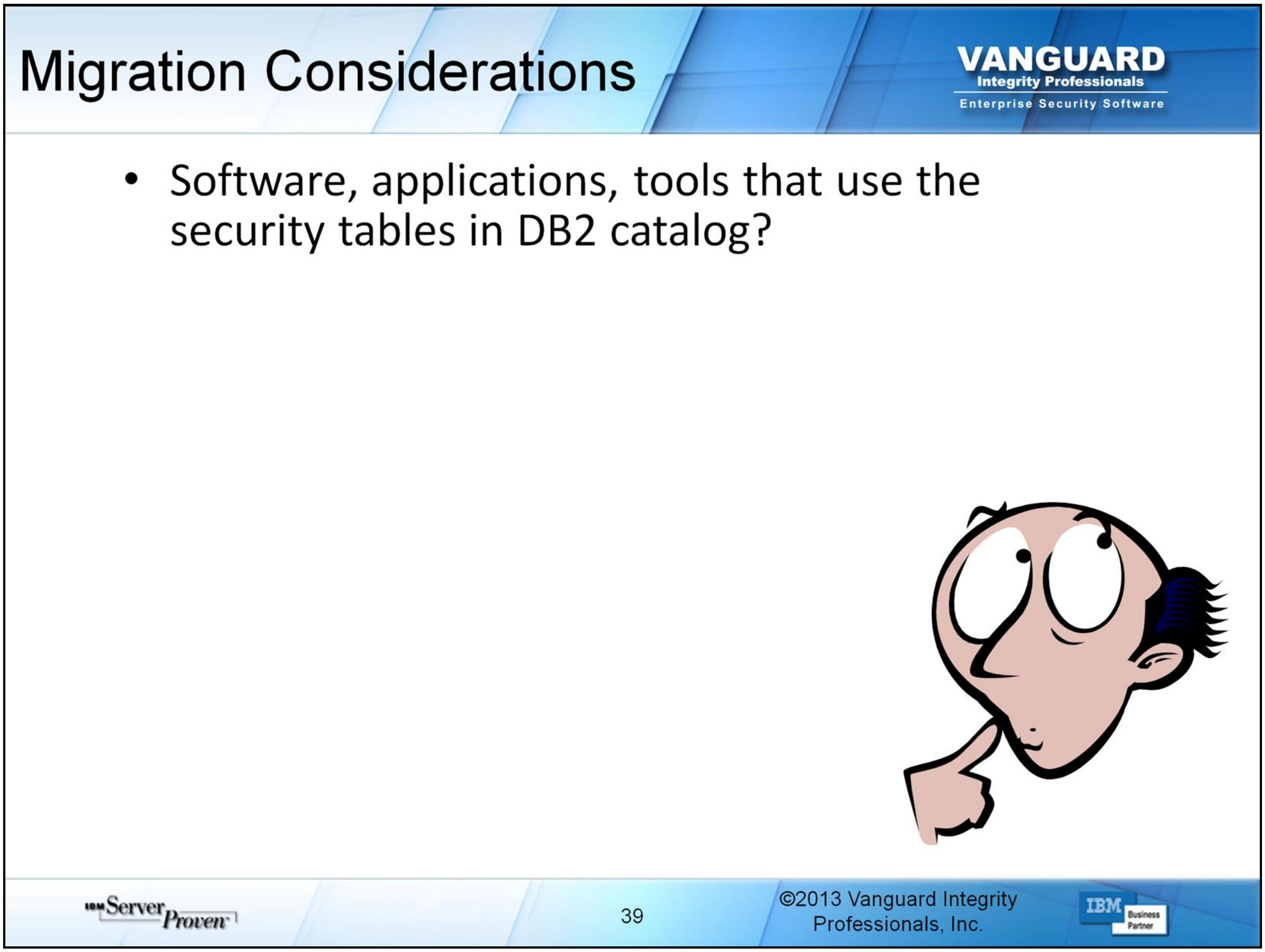
For CREATETMTAB, DB2 requires DBMAINT, DBCTRL, or DBADM. RACF checks for CREATETMTAB, CREATETAB, SYSCTRL, or SYSADM.

For the "any table" privilege:

In DB2, UPDATE and REFERENCES privilege for specific columns is sufficient for "any table"

In RACF, UPDATE and REFERENCES privilege for specific columns is not sufficient for "any table"

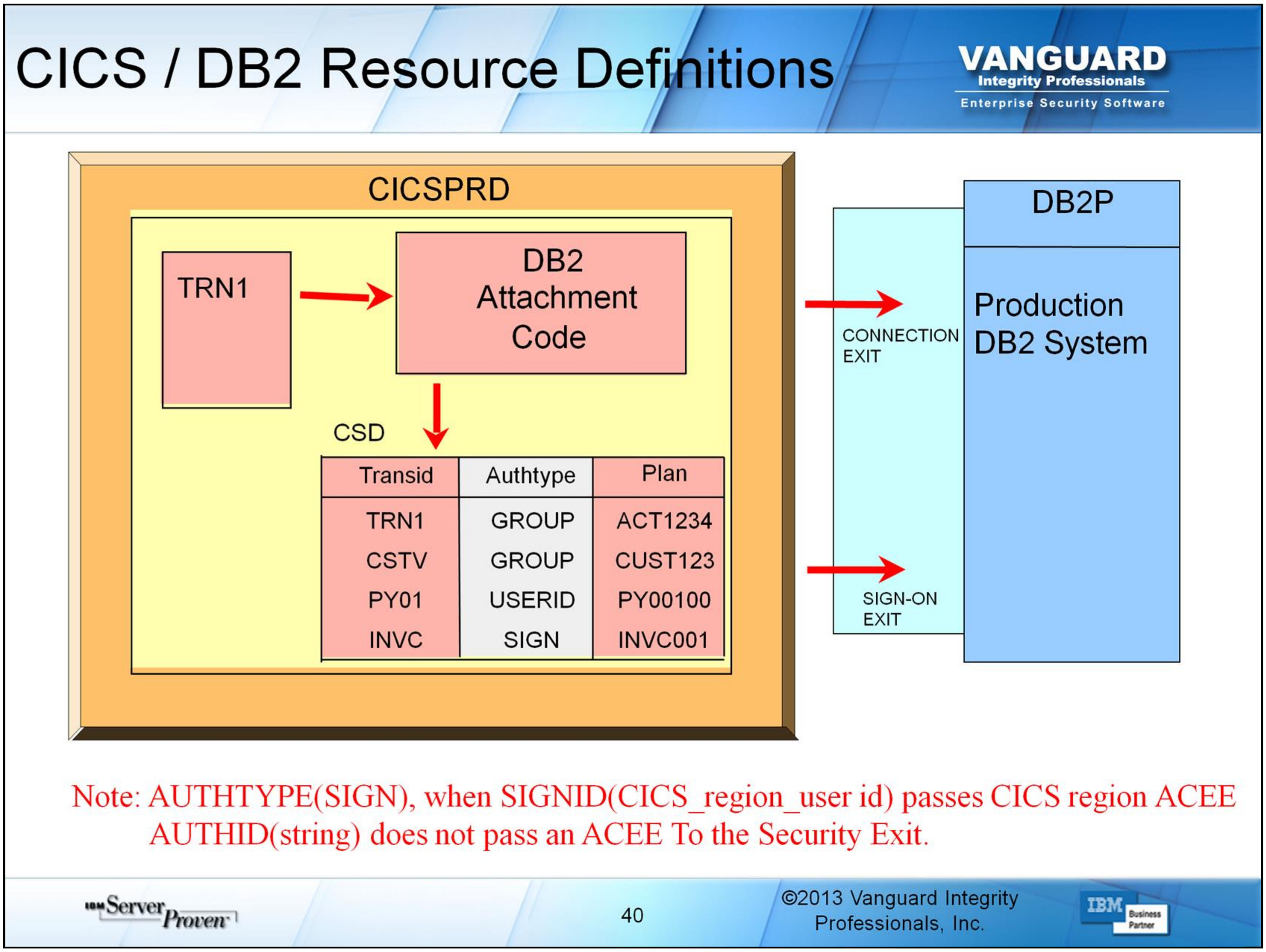
In DB2, a privilege can be GRANTed to a user WITH GRANT OPTION. This means the user can GRANT this privilege to others. RACF does not support this directly. However, if a user is placed in the access list of a discrete profile with ALTER access, that user could PERMIT other users.



Migration Considerations

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

After conversion to RACF, the SYSIBM.SYSxxxxAUTH tables will gradually become invalid, so any tools that read the DB2 auth tables will no longer be useful.



CICS / DB2 Resource Definitions

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

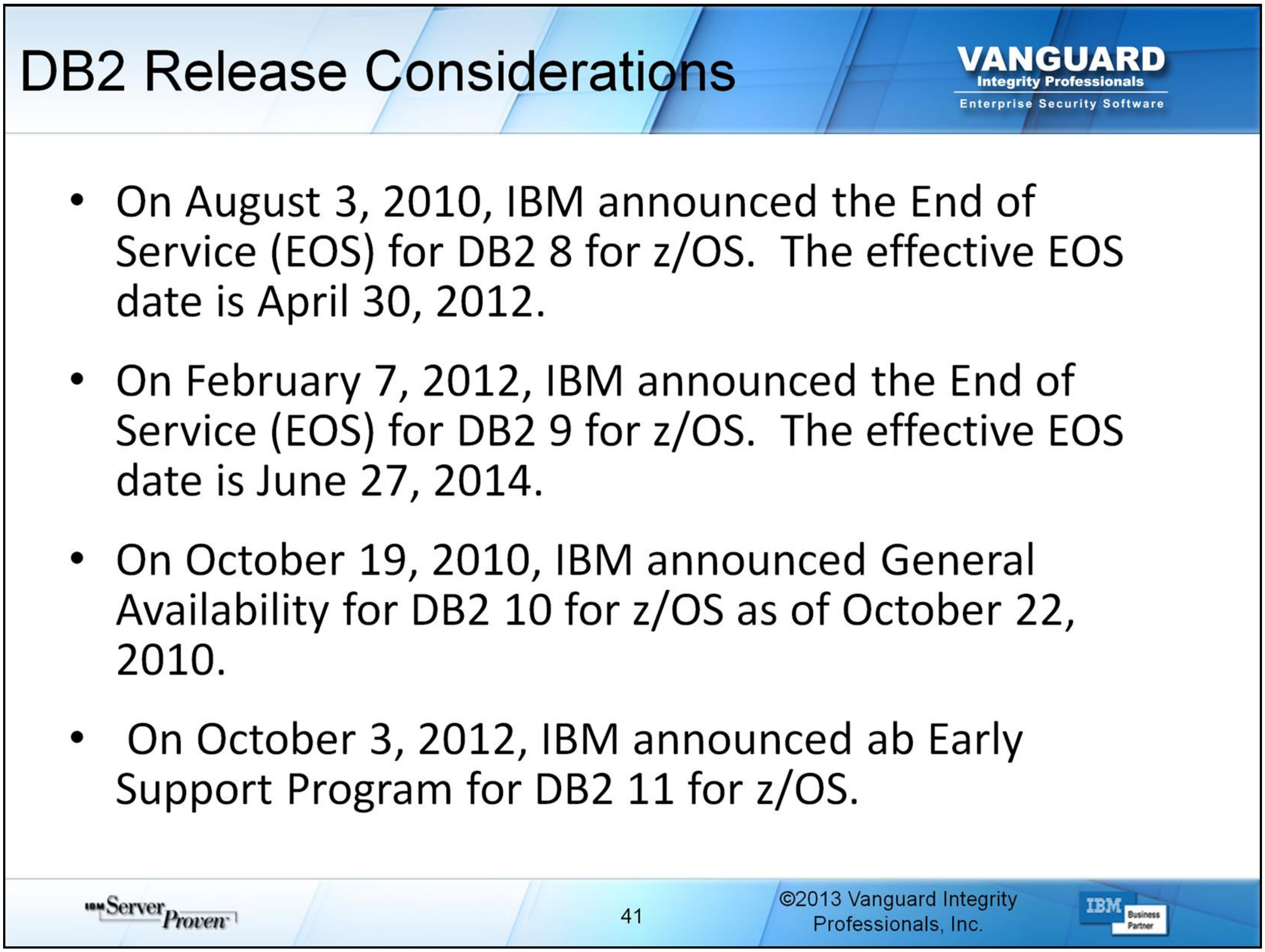
Note: AUTHTYPE(SIGN), when SIGNID(CICS_region_user id) passes CICS region ACEE
AUTHID(string) does not pass an ACEE To the Security Exit.

A DB2ENTRY definition specifies the attributes of entry threads used by the CICS DB2 attachment facility to a transaction. A group of transactions, can be associated with a DB2ENTRY definition by defining each additional transaction ID in a DB2TRAN definition naming the DB2ENTRY name.

If you are using RACF for some or all of the security checking in your DB2 address space, you need to use the USERID, GROUP, or SIGN options. This is because only threads defined with these options pass the required RACF access control environment element (ACEE) to DB2.

When the DB2 sample sign-on exit DSN3@SGN is used with AUTHTYPE(USERID), the exit sends the user ID to DB2 as the primary authorization ID and the connected group name to DB2 as the secondary ID. When the sample sign-on exit is used, there is no difference between AUTHTYPE(USERID) and AUTHTYPE(GROUP).

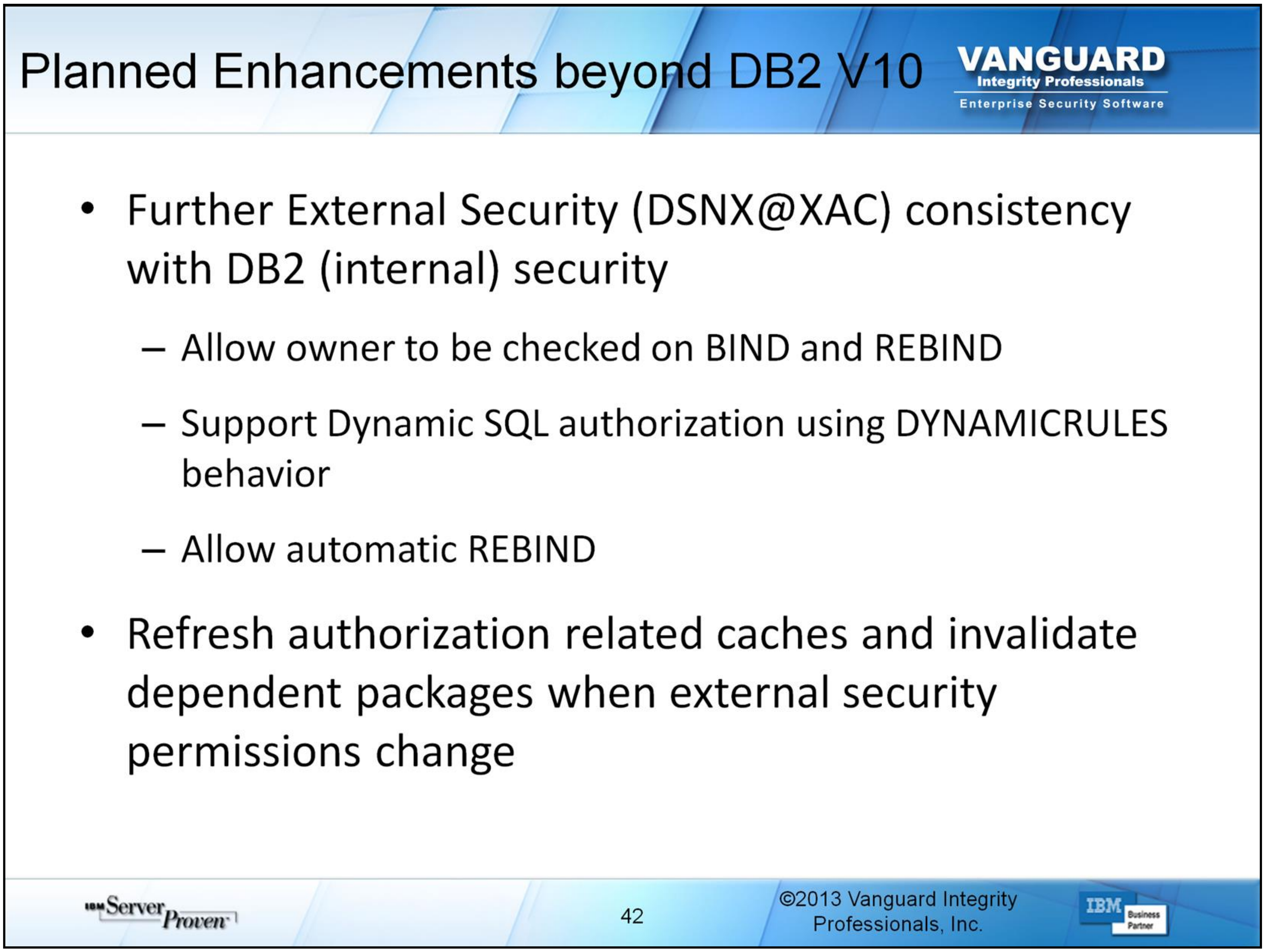
To use the GROUP option, the CICS system must have RACF external security SEC=YES specified in the CICS system initialization table (SIT).



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 ab Early Support Program for DB2 11 for z/OS.

The DB2 version in use will have only a minor effect on the migration to RACF for security, but there are a number of minor differences, some of which are unique to the particular DB2 version in use.



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

DB2 development is planning further enhancements to the RACF security facilities for DB2, but there is currently no commitment in which DB2 version or release any particular enhancement will first be introduced.

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!

VANGUARD
Integrity Professionals
Enterprise Security Software

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

Thank You
English

ขอบคุณ
Thai

شكراً
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

IBM Server Proven

©2013 Vanguard Integrity Professionals, Inc.

IBM Business Partner

This session was devoted to a discussion of the advantages and considerations that should be considered when contemplating or proposing a migration of security for DB2 from the security mechanisms internal to DB2 itself to security for DB2 based on profiles defined in a RACF database.

I hope that this session has provided information that will be helpful for you to evaluate the value within your organization of migrating security for DB2 to RACF.

Please ask any questions that come to mind concerning any considerations related to this migration process that were not clearly covered or appear to have been omitted.