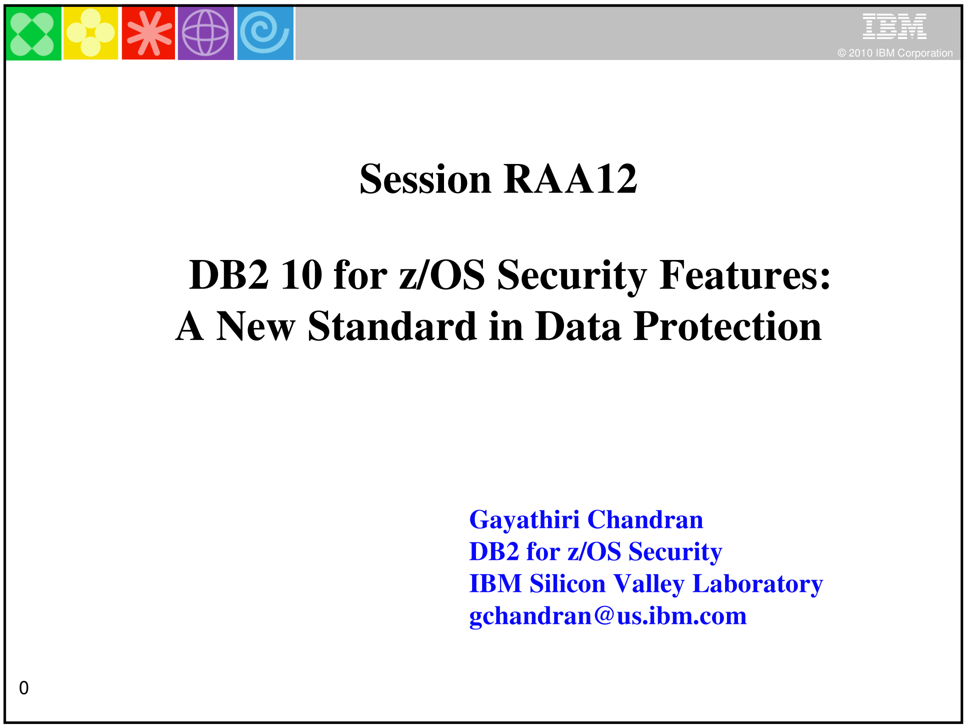
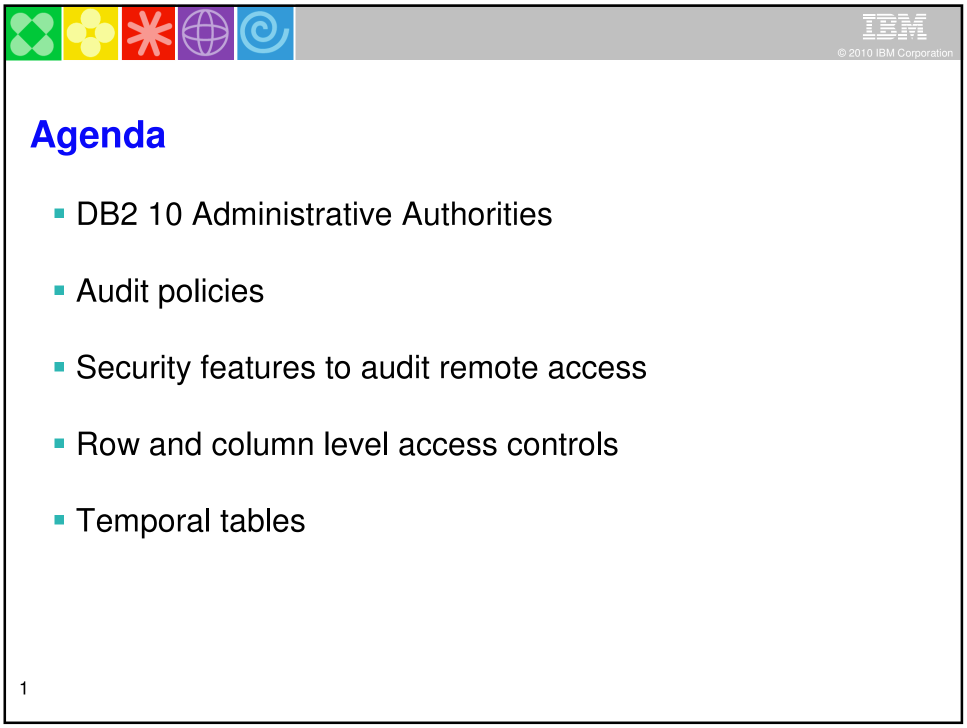


Session RAA12

DB2 10 for z/OS Security Features:
A New Standard in Data Protection

Gayathiri Chandran
DB2 for z/OS Security
IBM Silicon Valley Laboratory
gchandran@us.ibm.com

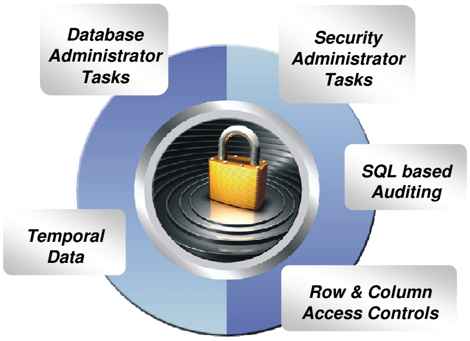


Agenda

- DB2 10 Administrative Authorities
- Audit policies
- Security features to audit remote access
- Row and column level access controls
- Temporal tables

Satisfy Your Auditor: Plan, Protect and Audit

- Data Access
  - Minimize the use of a superuser authorities such as SYSADM
  - A different group should manage access to restricted data than the owner of the data
- Data Auditing
  - Any dynamic access or use of a privileged authority needs to be included in your audit trail
  - Maintain historical versions of data for years or during a business period
- Data Privacy
  - All dynamic access to tables containing restricted data needs to be protected


Database Administrator Tasks
Security Administrator Tasks
SQL based Auditing
Temporal Data
Row & Column Access Controls

Today's Mainframe:
The power of industry-leading security,
the simplicity of centralised management

Reduce risk by minimizing use of SYSADM

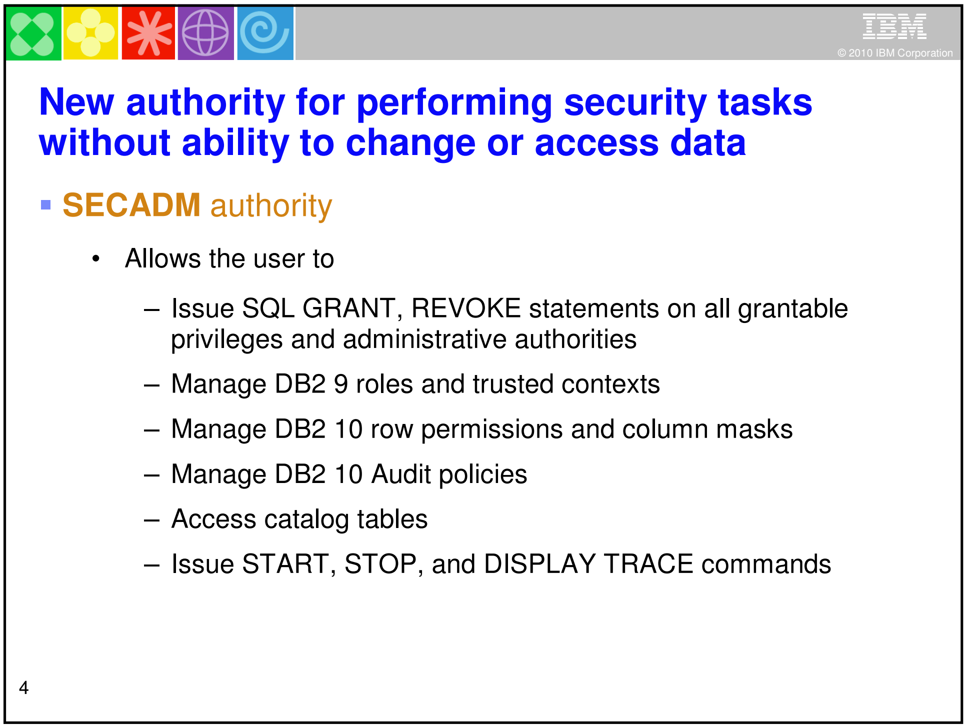
New granular system authorities

Prior to DB2 10

- **SYSADM**
- **DBADM**
- **DBCTRL**
- **DBMAINT**
- **SYSCTRL**
- **PACKADM**
- **SYSOPR**

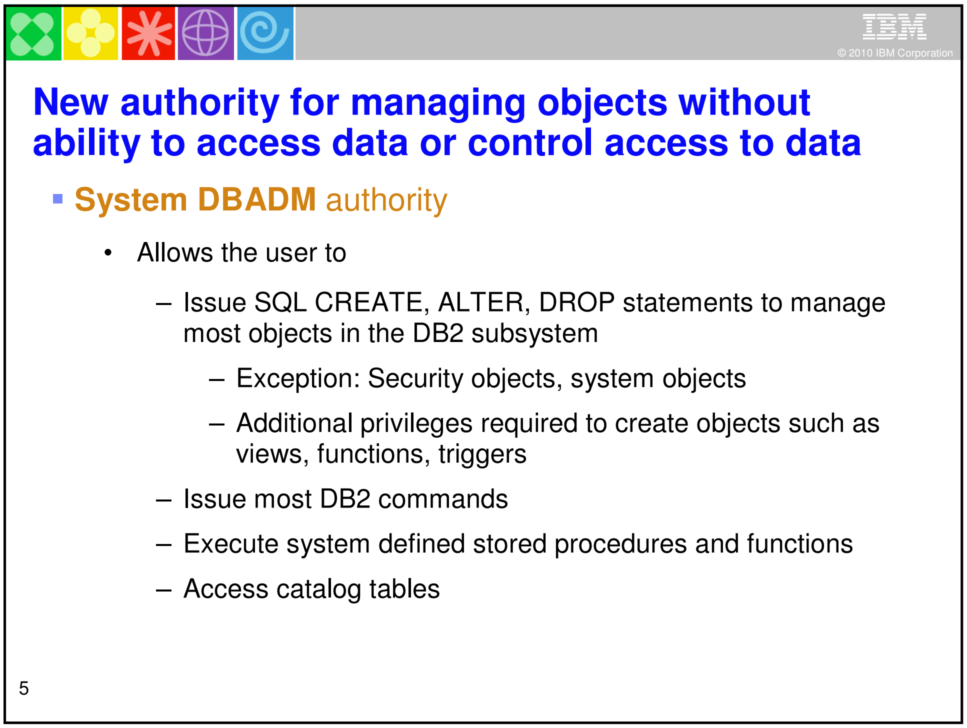
New in DB2 10

- **System DBADM**
- **ACCESSCTRL**
- **DATAACCESS**
- **SECADM**
- **SQLADM**
- **EXPLAIN**



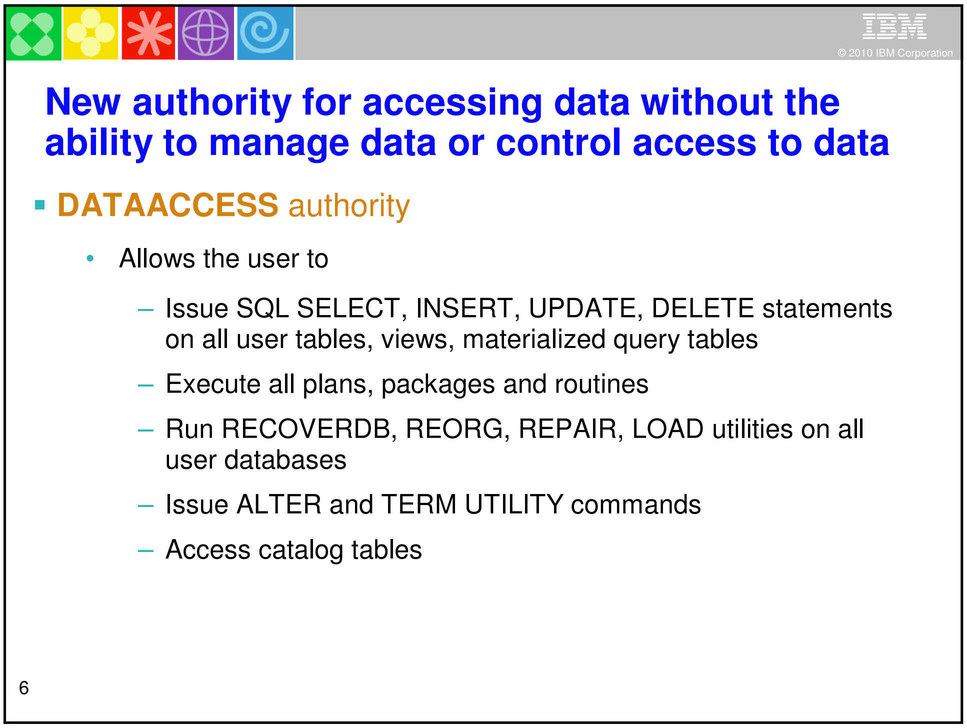
New authority for performing security tasks without ability to change or access data

- **SECADM** authority
  - Allows the user to
    - Issue SQL GRANT, REVOKE statements on all grantable privileges and administrative authorities
    - Manage DB2 9 roles and trusted contexts
    - Manage DB2 10 row permissions and column masks
    - Manage DB2 10 Audit policies
    - Access catalog tables
    - Issue START, STOP, and DISPLAY TRACE commands



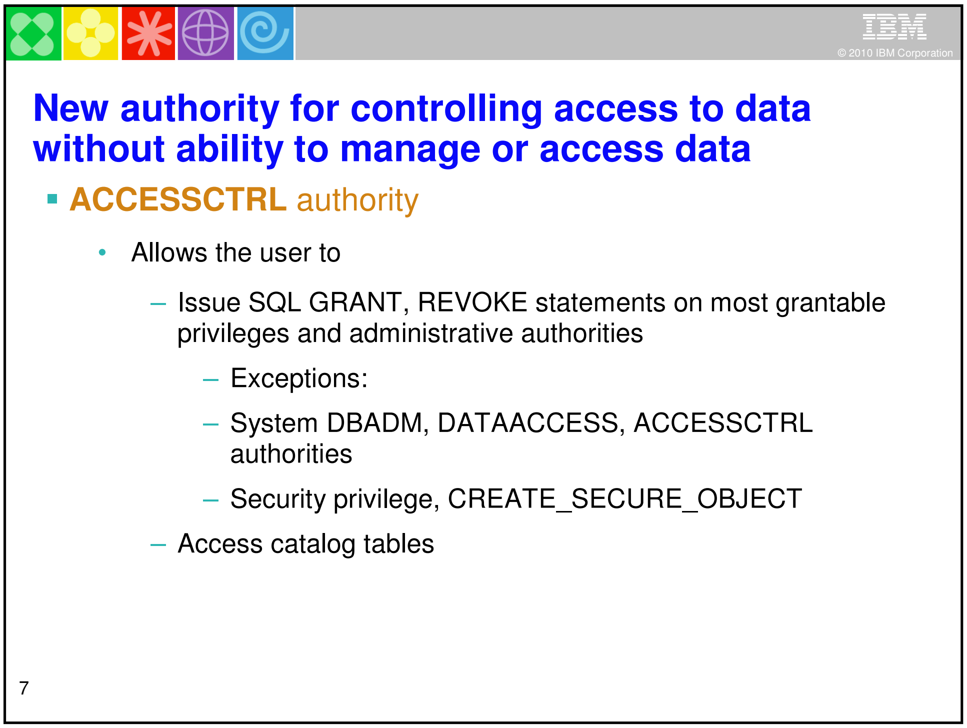
New authority for managing objects without ability to access data or control access to data

- **System DBADM** authority
  - Allows the user to
    - Issue SQL CREATE, ALTER, DROP statements to manage most objects in the DB2 subsystem
      - Exception: Security objects, system objects
      - Additional privileges required to create objects such as views, functions, triggers
    - Issue most DB2 commands
    - Execute system defined stored procedures and functions
    - Access catalog tables



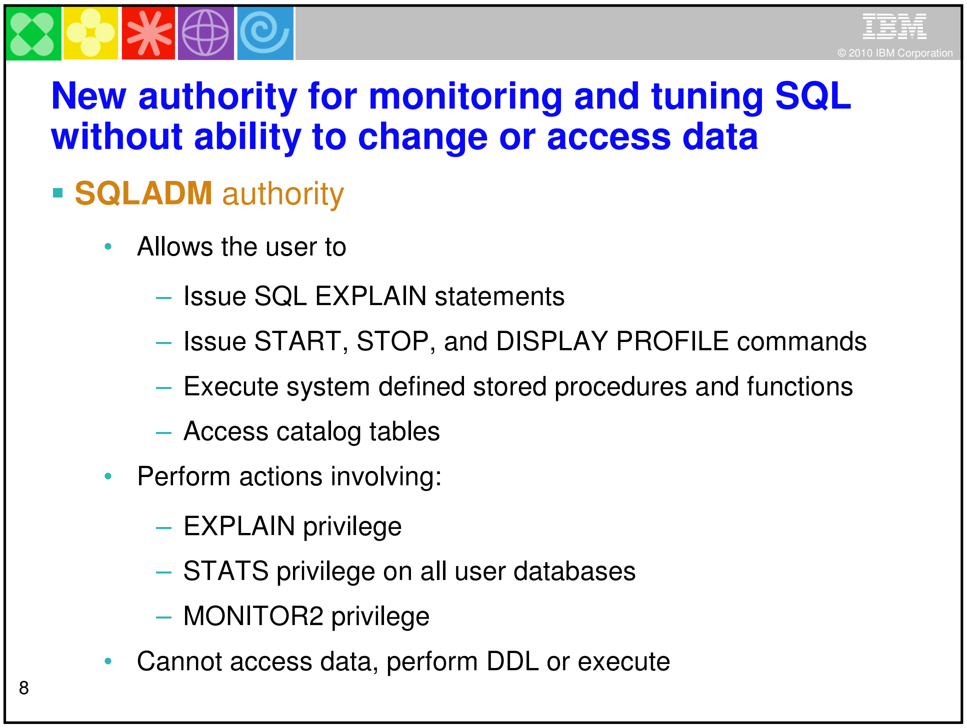
New authority for accessing data without the ability to manage data or control access to data

- **DATAACCESS** authority
  - Allows the user to
    - Issue SQL SELECT, INSERT, UPDATE, DELETE statements on all user tables, views, materialized query tables
    - Execute all plans, packages and routines
    - Run RECOVERDB, REORG, REPAIR, LOAD utilities on all user databases
    - Issue ALTER and TERM UTILITY commands
    - Access catalog tables



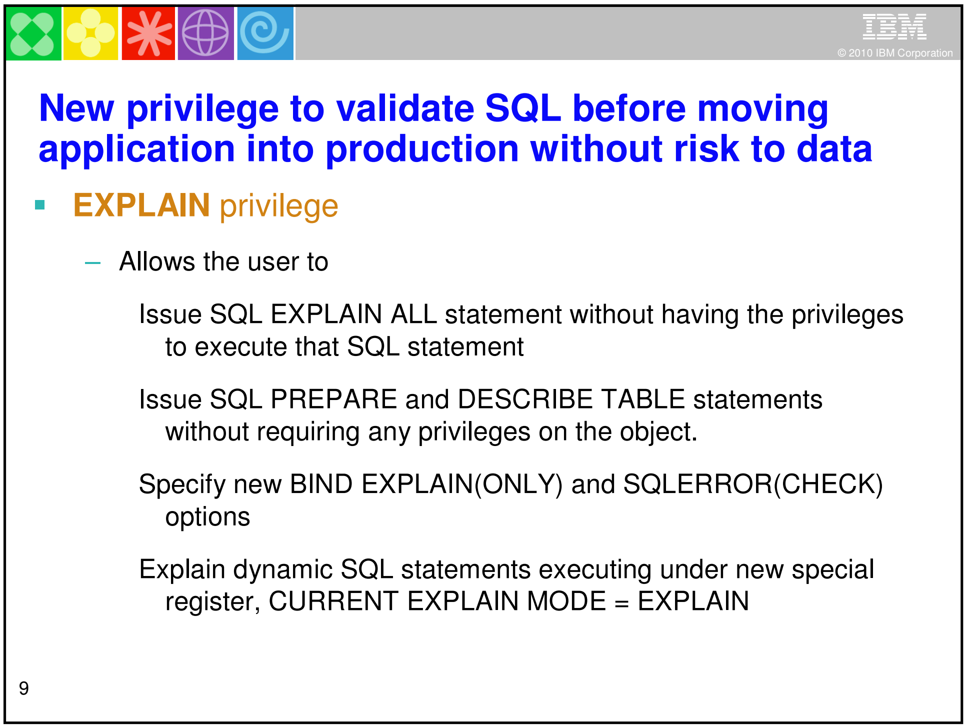
New authority for controlling access to data without ability to manage or access data

- **ACCESSCTRL** authority
  - Allows the user to
    - Issue SQL GRANT, REVOKE statements on most grantable privileges and administrative authorities
      - Exceptions:
      - System DBADM, DATAACCESS, ACCESSCTRL authorities
      - Security privilege, CREATE_SECURE_OBJECT
    - Access catalog tables



New authority for monitoring and tuning SQL without ability to change or access data

- **SQLADM** authority
  - Allows the user to
    - Issue SQL EXPLAIN statements
    - Issue START, STOP, and DISPLAY PROFILE commands
    - Execute system defined stored procedures and functions
    - Access catalog tables
  - Perform actions involving:
    - EXPLAIN privilege
    - STATS privilege on all user databases
    - MONITOR2 privilege
  - Cannot access data, perform DDL or execute



New privilege to validate SQL before moving application into production without risk to data

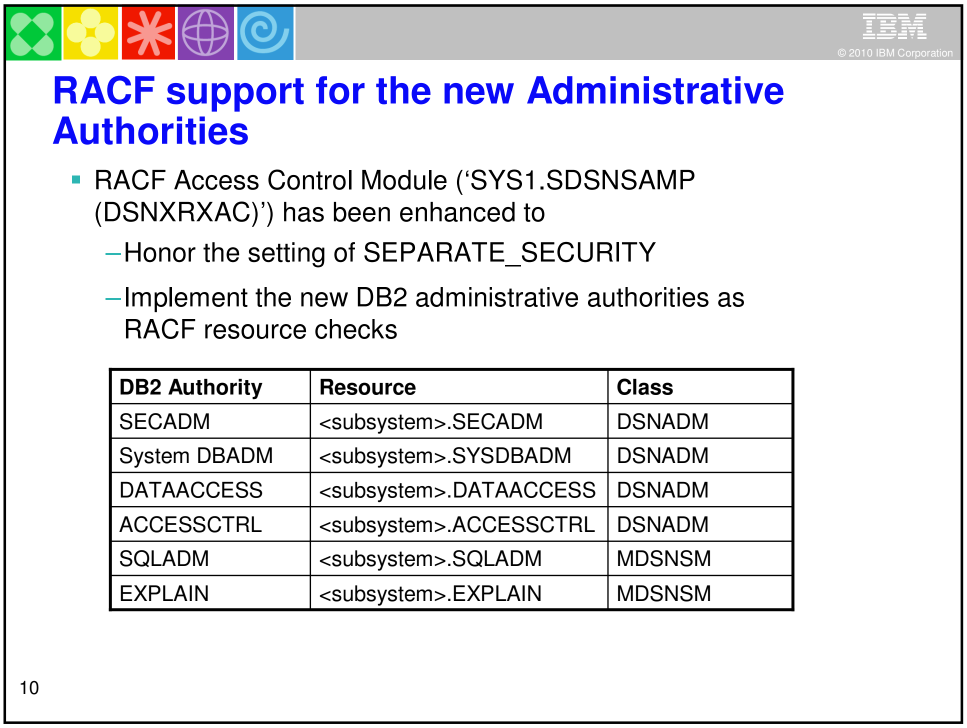
- **EXPLAIN** privilege
  - Allows the user to

    Issue SQL EXPLAIN ALL statement without having the privileges to execute that SQL statement

    Issue SQL PREPARE and DESCRIBE TABLE statements without requiring any privileges on the object.

    Specify new BIND EXPLAIN(ONLY) and SQLERROR(CHECK) options

    Explain dynamic SQL statements executing under new special register, CURRENT EXPLAIN MODE = EXPLAIN

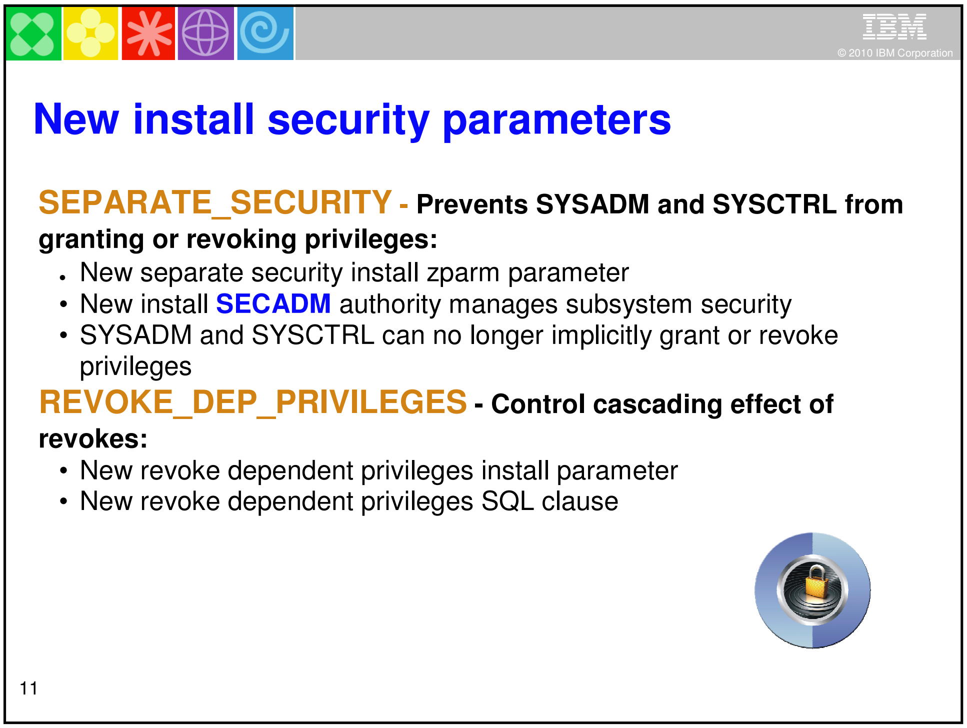


RACF support for the new Administrative Authorities

- RACF Access Control Module (‘SYS1.SDSNSAMP (DSNXRXAC)’) has been enhanced to
  - Honor the setting of SEPARATE_SECURITY
  - Implement the new DB2 administrative authorities as RACF resource checks

DB2 Authority	Resource	Class
SECADM	<subsystem>.SECADM	DSNADM
System DBADM	<subsystem>.SYSDBADM	DSNADM
DATAACCESS	<subsystem>.DATAACCESS	DSNADM
ACCESSCTRL	<subsystem>.ACCESSCTRL	DSNADM
SQLADM	<subsystem>.SQLADM	MDSNSM
EXPLAIN	<subsystem>.EXPLAIN	MDSNSM

10



New install security parameters

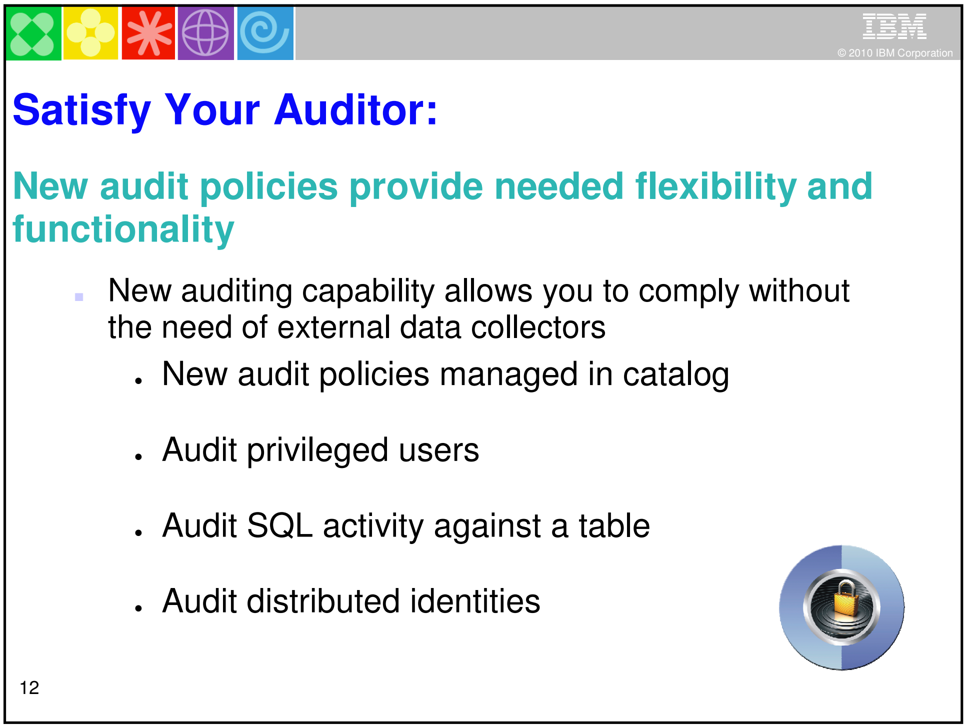
SEPARATE_SECURITY - Prevents SYSADM and SYSCTRL from granting or revoking privileges:

- New separate security install zparm parameter
- New install **SECADM** authority manages subsystem security
- SYSADM and SYSCTRL can no longer implicitly grant or revoke privileges

REVOKE_DEP_PRIVILEGES - Control cascading effect of revokes:

- New revoke dependent privileges install parameter
- New revoke dependent privileges SQL clause

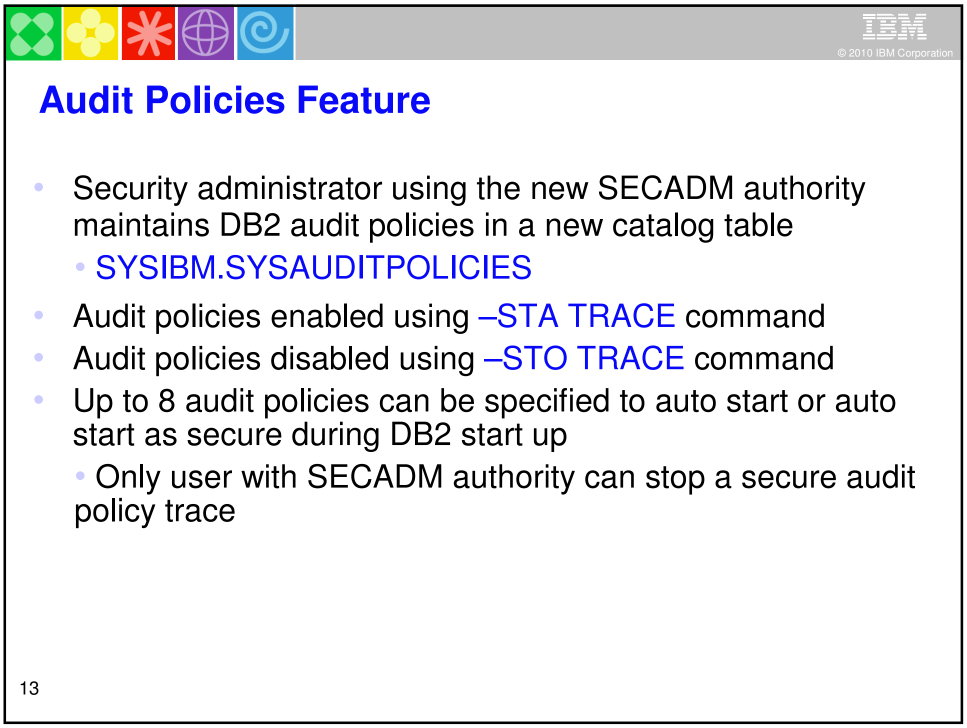
11



Satisfy Your Auditor:

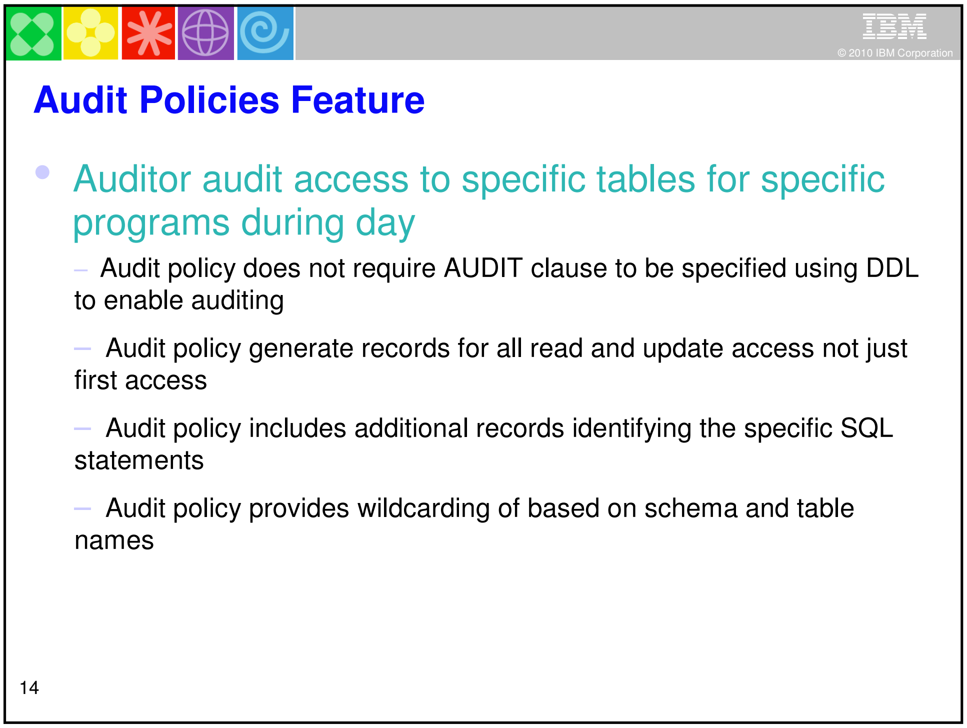
New audit policies provide needed flexibility and functionality

- New auditing capability allows you to comply without the need of external data collectors
  - New audit policies managed in catalog
  - Audit privileged users
  - Audit SQL activity against a table
  - Audit distributed identities



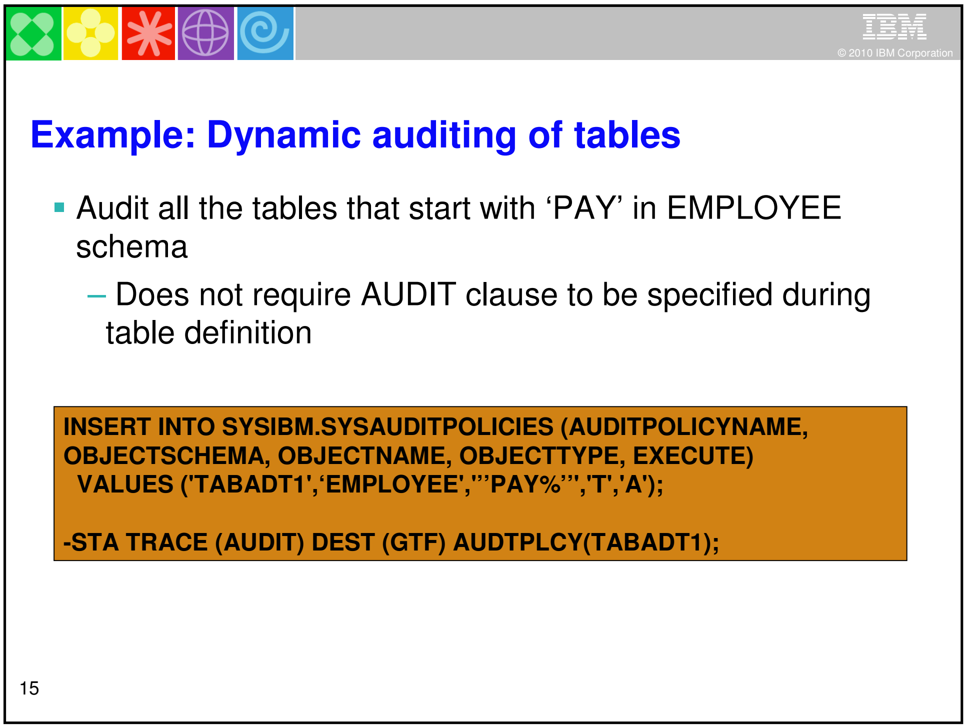
Audit Policies Feature

- Security administrator using the new SECADM authority maintains DB2 audit policies in a new catalog table
  - SYSIBM.SYSAUDITPOLICIES
- Audit policies enabled using –STA TRACE command
- Audit policies disabled using –STO TRACE command
- Up to 8 audit policies can be specified to auto start or auto start as secure during DB2 start up
  - Only user with SECADM authority can stop a secure audit policy trace



Audit Policies Feature

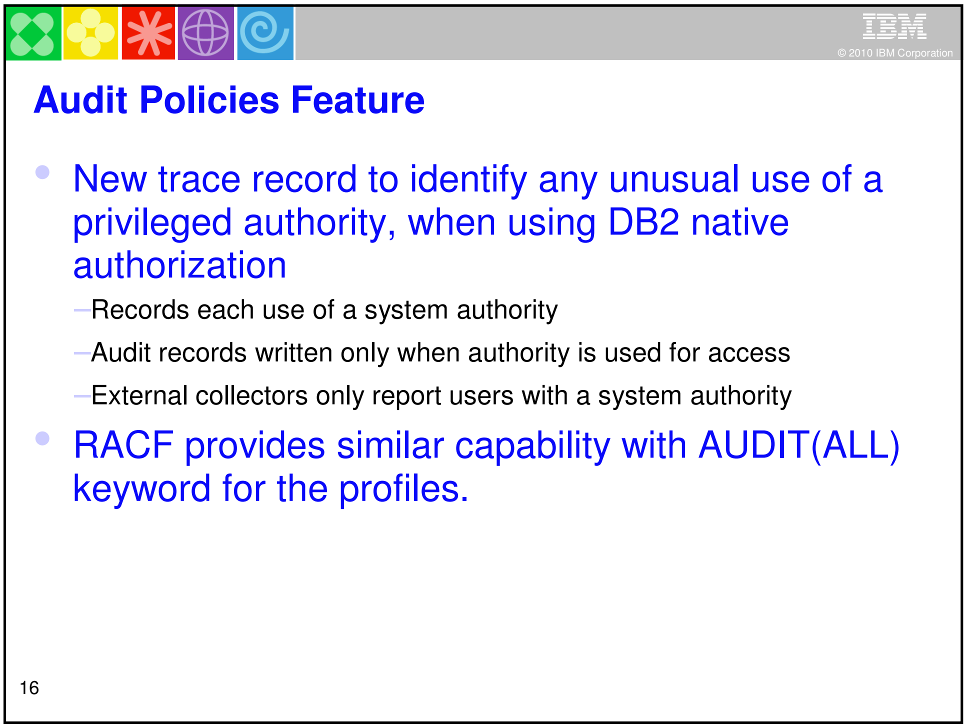
- Auditor audit access to specific tables for specific programs during day
  - Audit policy does not require AUDIT clause to be specified using DDL to enable auditing
  - Audit policy generate records for all read and update access not just first access
  - Audit policy includes additional records identifying the specific SQL statements
  - Audit policy provides wildcarding of based on schema and table names



Example: Dynamic auditing of tables

- Audit all the tables that start with ‘PAY’ in EMPLOYEE schema
  - Does not require AUDIT clause to be specified during table definition

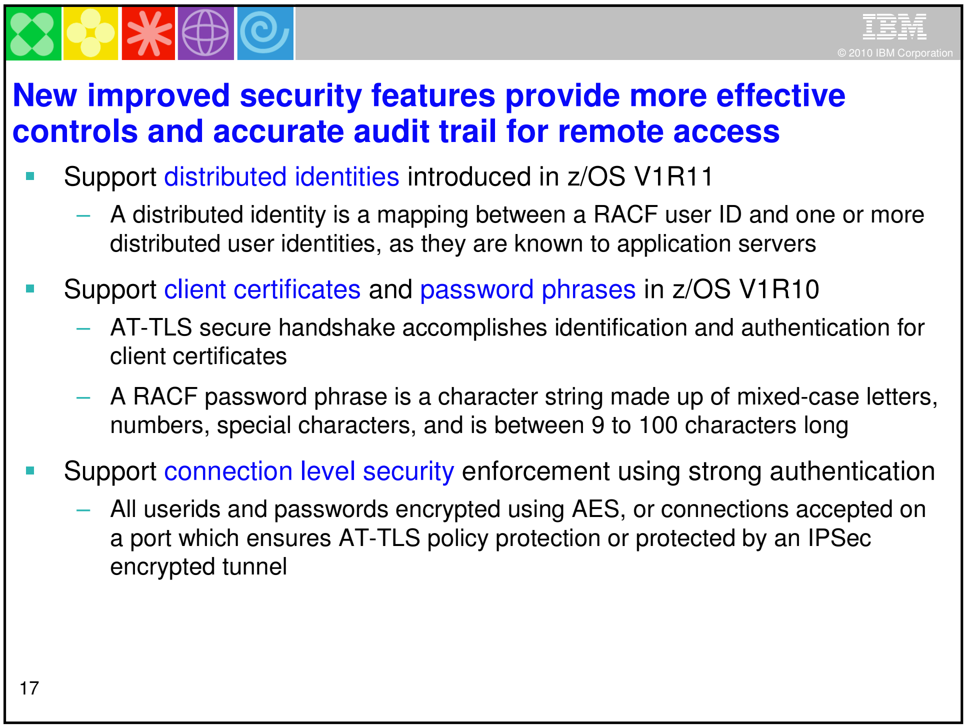
```
INSERT INTO SYSIBM.SYSAUDITPOLICIES (AUDITPOLICYNAME,
OBJECTSCHEMA, OBJECTNAME, OBJECTTYPE, EXECUTE)
  VALUES ('TABADT1',‘EMPLOYEE','’’PAY%’’','T','A');

-STA TRACE (AUDIT) DEST (GTF) AUDTPLCY(TABADT1);
```



Audit Policies Feature

- New trace record to identify any unusual use of a privileged authority, when using DB2 native authorization
  - Records each use of a system authority
  - Audit records written only when authority is used for access
  - External collectors only report users with a system authority
- RACF provides similar capability with AUDIT(ALL) keyword for the profiles.

16



New improved security features provide more effective controls and accurate audit trail for remote access

- Support distributed identities introduced in z/OS V1R11
  - A distributed identity is a mapping between a RACF user ID and one or more distributed user identities, as they are known to application servers
- Support client certificates and password phrases in z/OS V1R10
  - AT-TLS secure handshake accomplishes identification and authentication for client certificates
  - A RACF password phrase is a character string made up of mixed-case letters, numbers, special characters, and is between 9 to 100 characters long
- Support connection level security enforcement using strong authentication
  - All userids and passwords encrypted using AES, or connections accepted on a port which ensures AT-TLS policy protection or protected by an IPSec encrypted tunnel

17

Satisfy Your Auditor:

New table controls to protect against unplanned SQL access

- Define additional data controls at the row and column level
  - Security policies are defined using SQL
  - Separate security logic from application logic
- Security policies based on real time session attributes
  - Protects against SQL injection attacks
  - Determines how column values are returned
  - Determines which rows are returned
- All access via SQL including privileged users, adhoc query tools, report generation tools is protected
- Policies can be added, modified, or removed to meet current company rules without change to applications

Table controls to protect SQL access to individual row level

Establish a row policy for a table

- Filter rows out of answer set
- Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control which row is returned in result set
- Applicable to SELECT, INSERT, UPDATE, DELETE, & MERGE
- Defined as a row permission:

```
CREATE PERMISSION policy-name ON table-name
    FOR ROWS WHERE search-condition
    ENFORCED FOR ALL ACCESS ENABLE;
```

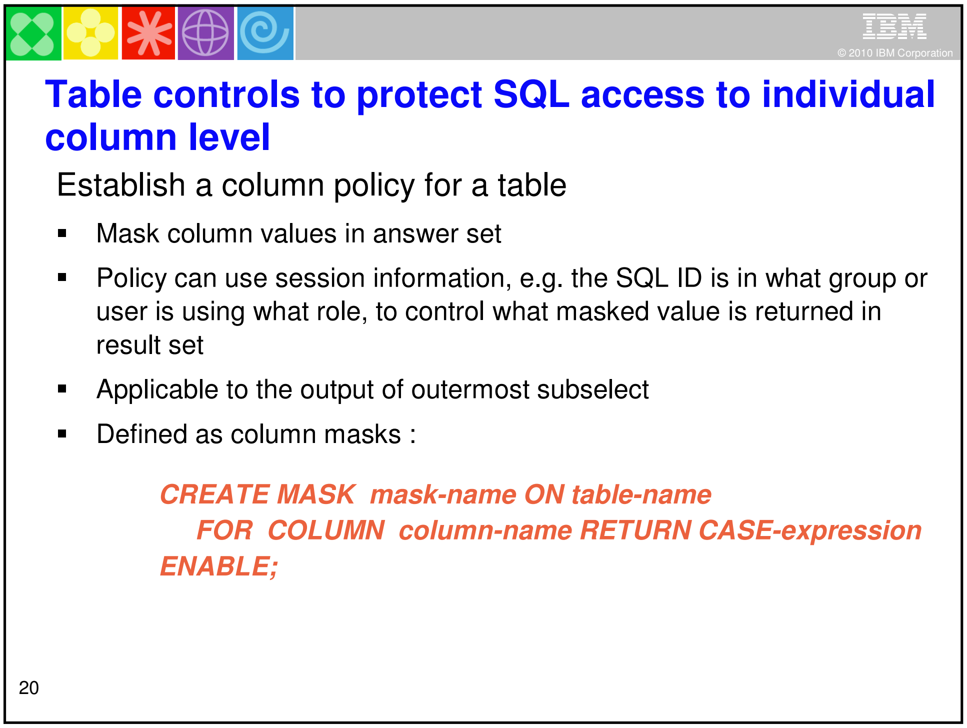
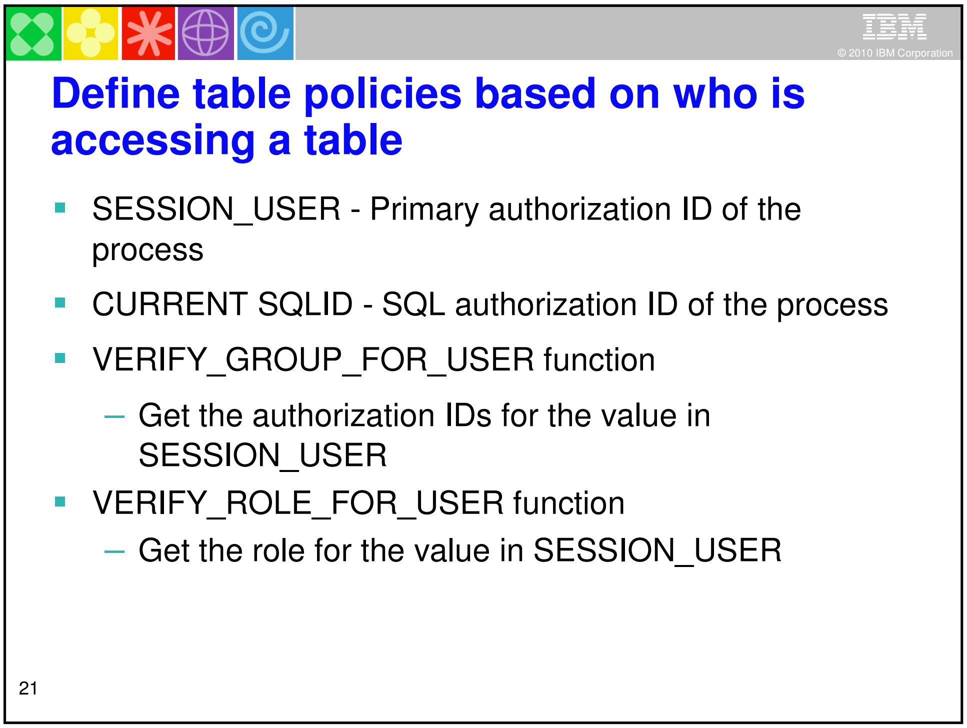


Table controls to protect SQL access to individual column level

Establish a column policy for a table

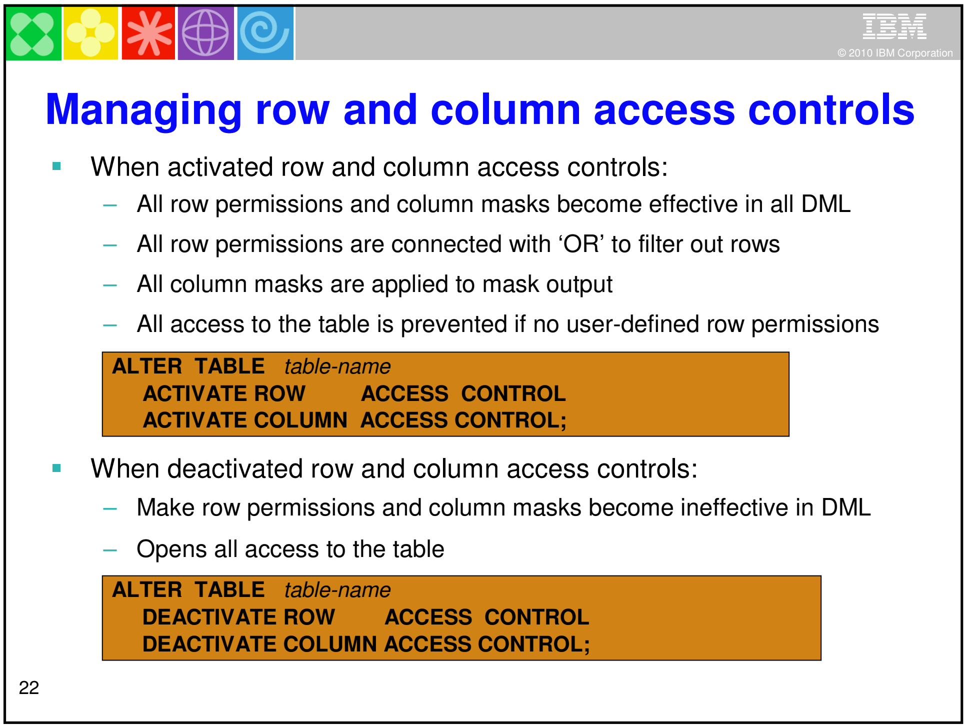
- Mask column values in answer set
- Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control what masked value is returned in result set
- Applicable to the output of outermost subselect
- Defined as column masks :

```
CREATE MASK  mask-name ON table-name
    FOR  COLUMN  column-name RETURN CASE-expression
ENABLE;
```



Define table policies based on who is accessing a table

- SESSION_USER - Primary authorization ID of the process
- CURRENT SQLID - SQL authorization ID of the process
- VERIFY_GROUP_FOR_USER function
  - Get the authorization IDs for the value in SESSION_USER
- VERIFY_ROLE_FOR_USER function
  - Get the role for the value in SESSION_USER



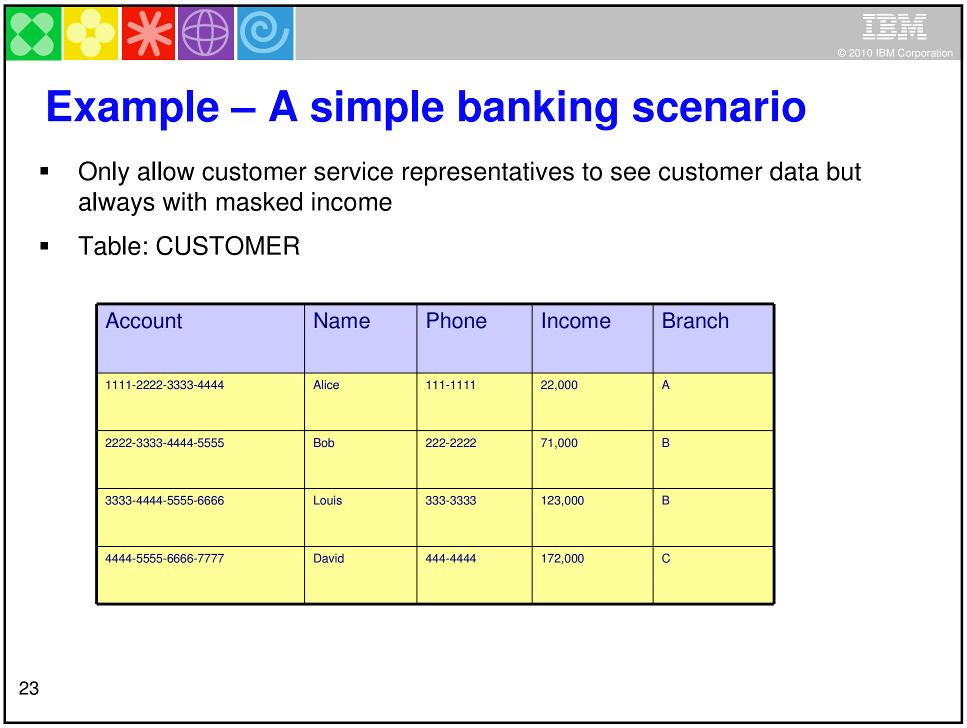
Managing row and column access controls

- When activated row and column access controls:
  - All row permissions and column masks become effective in all DML
  - All row permissions are connected with ‘OR’ to filter out rows
  - All column masks are applied to mask output
  - All access to the table is prevented if no user-defined row permissions

```
ALTER  TABLE   table-name
    ACTIVATE ROW         ACCESS  CONTROL
    ACTIVATE COLUMN  ACCESS CONTROL;
```

- When deactivated row and column access controls:
  - Make row permissions and column masks become ineffective in DML
  - Opens all access to the table

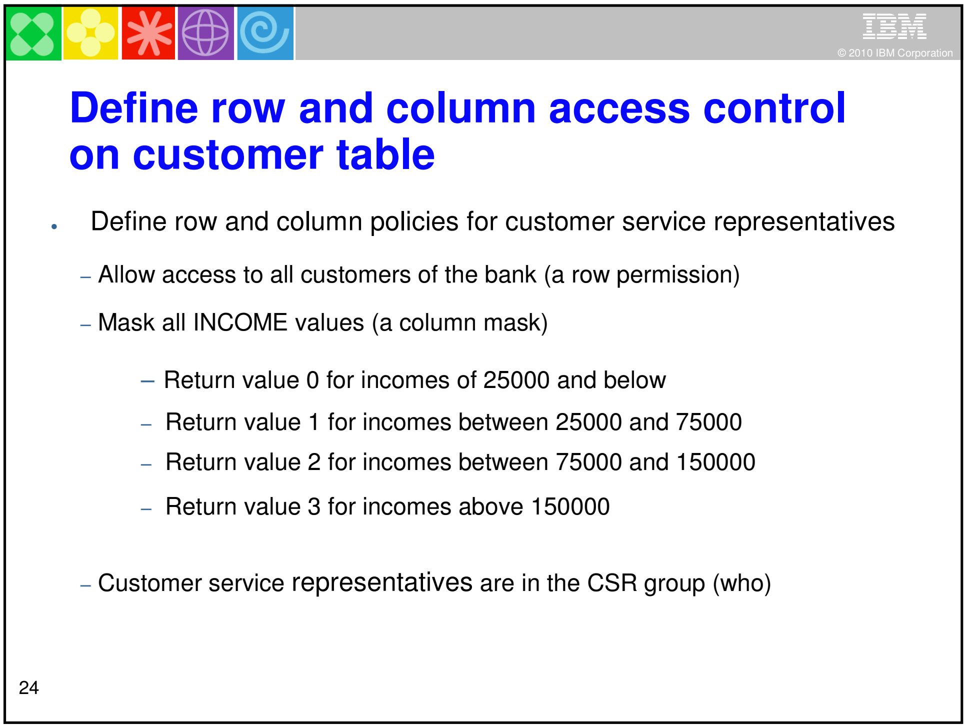
```
ALTER  TABLE   table-name
    DEACTIVATE ROW        ACCESS  CONTROL
    DEACTIVATE COLUMN ACCESS CONTROL;
```



Example – A simple banking scenario

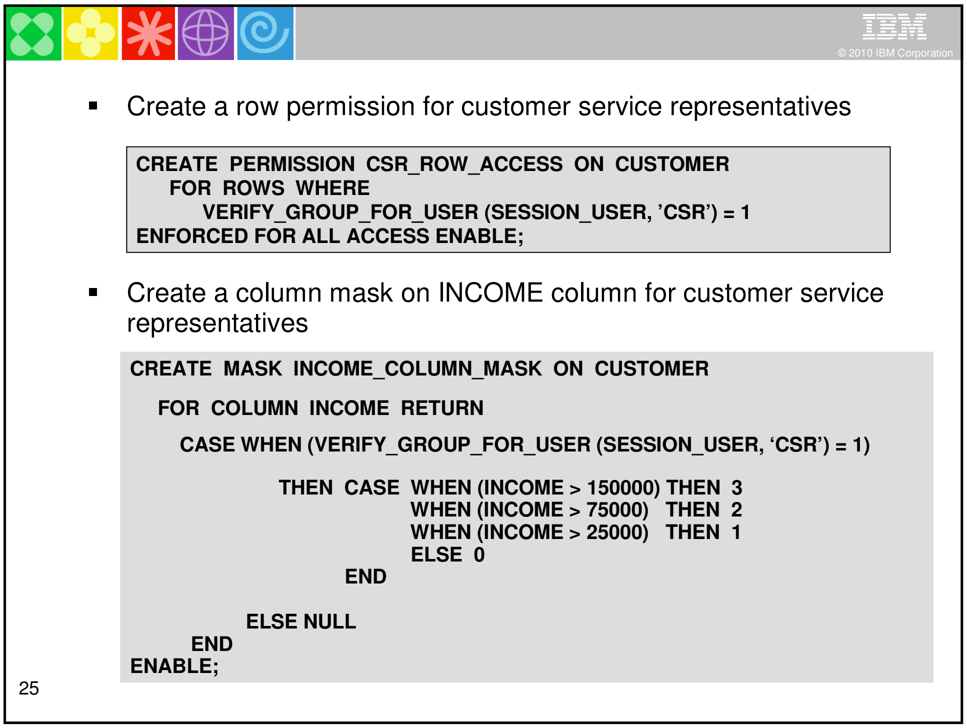
- Only allow customer service representatives to see customer data but always with masked income
- Table: CUSTOMER

Account	Name	Phone	Income	Branch
1111-2222-3333-4444	Alice	111-1111	22,000	A
2222-3333-4444-5555	Bob	222-2222	71,000	B
3333-4444-5555-6666	Louis	333-3333	123,000	B
4444-5555-6666-7777	David	444-4444	172,000	C



Define row and column access control on customer table

- Define row and column policies for customer service representatives
  - Allow access to all customers of the bank (a row permission)
  - Mask all INCOME values (a column mask)
    - Return value 0 for incomes of 25000 and below
    - Return value 1 for incomes between 25000 and 75000
    - Return value 2 for incomes between 75000 and 150000
    - Return value 3 for incomes above 150000
  - Customer service representatives are in the CSR group (who)

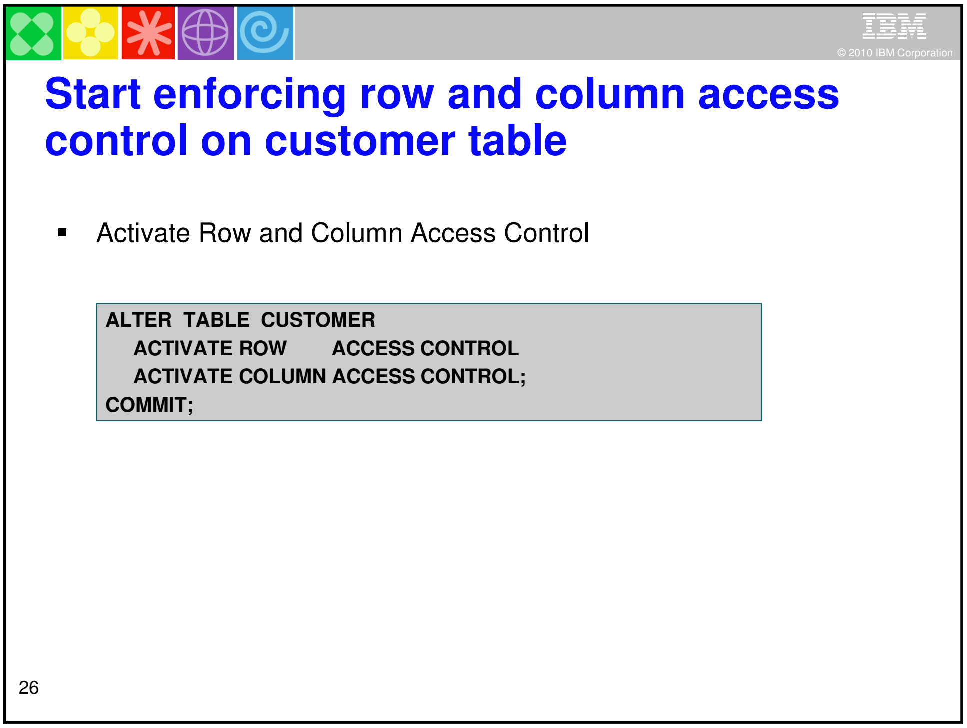


- Create a row permission for customer service representatives

```
CREATE  PERMISSION  CSR_ROW_ACCESS  ON  CUSTOMER
    FOR  ROWS  WHERE
        VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1
ENFORCED FOR ALL ACCESS ENABLE;
```

- Create a column mask on INCOME column for customer service representatives

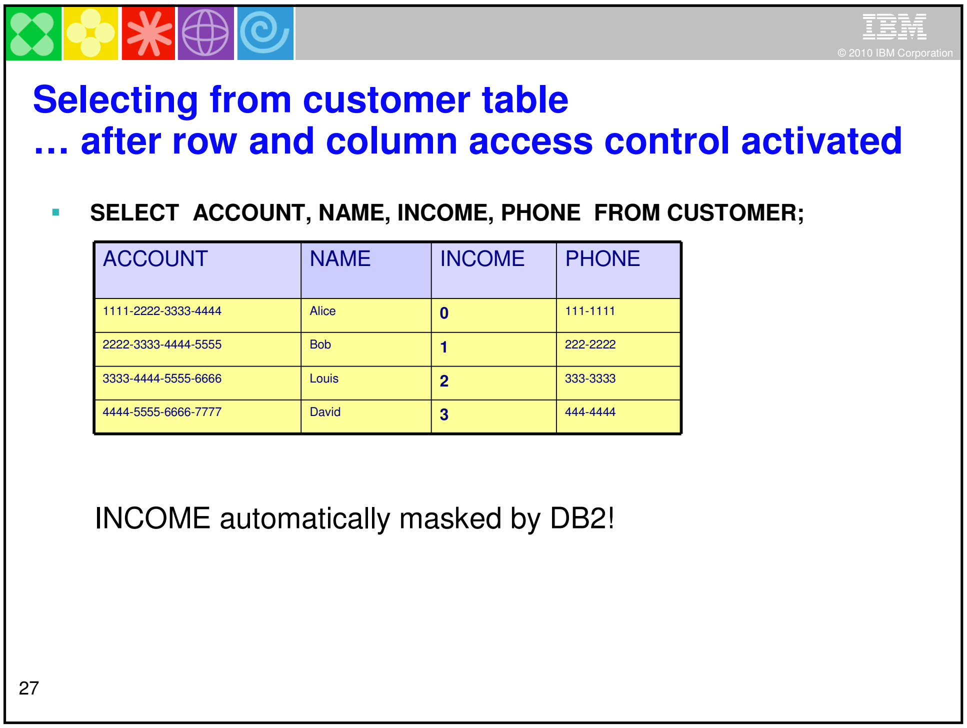
```
CREATE  MASK  INCOME_COLUMN_MASK  ON  CUSTOMER

   FOR  COLUMN  INCOME  RETURN

     CASE WHEN (VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1)

                THEN  CASE  WHEN (INCOME > 150000) THEN  3
                            WHEN (INCOME > 75000)   THEN  2
                            WHEN (INCOME > 25000)   THEN  1
                            ELSE  0
                      END

             ELSE NULL
        END
ENABLE;
```



Start enforcing row and column access control on customer table

- Activate Row and Column Access Control

```
ALTER  TABLE  CUSTOMER
    ACTIVATE ROW        ACCESS CONTROL
    ACTIVATE COLUMN ACCESS CONTROL;
COMMIT;
```

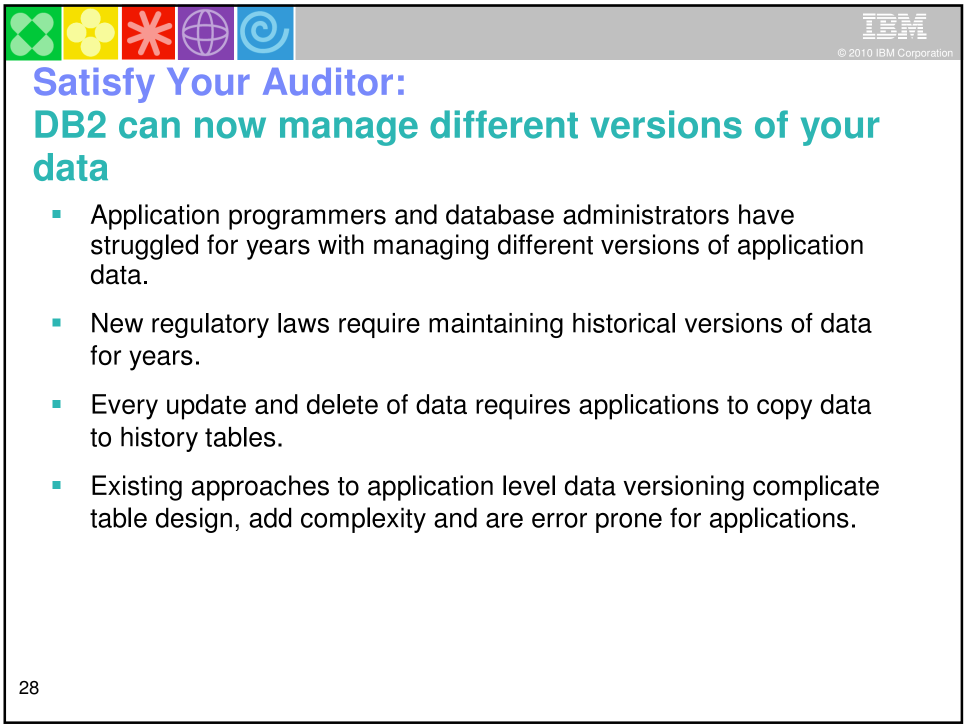


Selecting from customer table
… after row and column access control activated

- **SELECT ACCOUNT, NAME, INCOME, PHONE FROM CUSTOMER;**

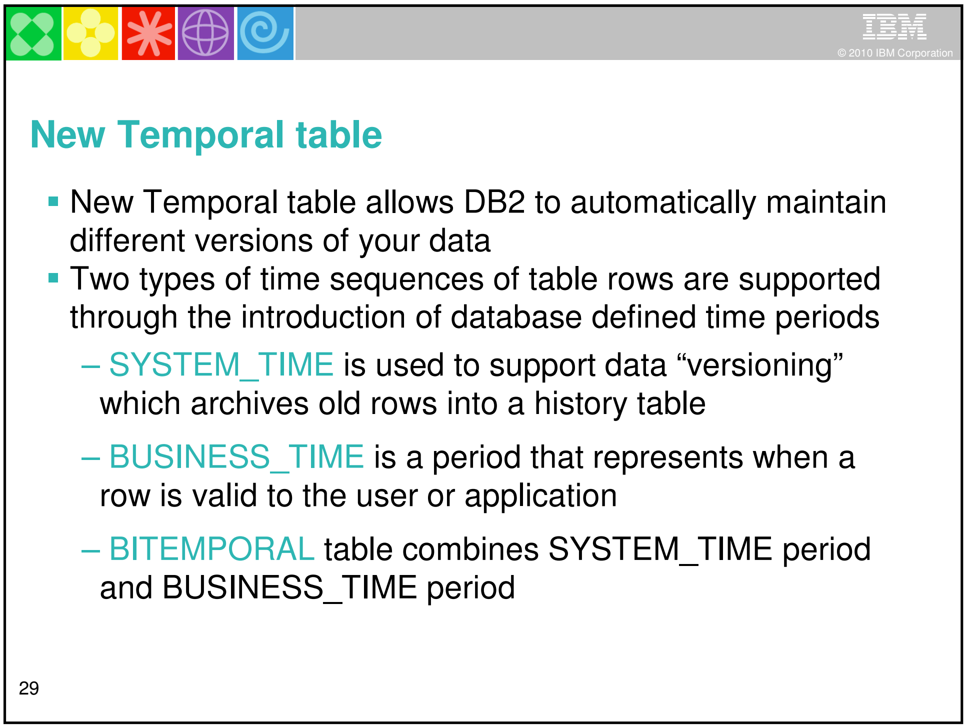
ACCOUNT	NAME	INCOME	PHONE
1111-2222-3333-4444	Alice	**0**	111-1111
2222-3333-4444-5555	Bob	**1**	222-2222
3333-4444-5555-6666	Louis	**2**	333-3333
4444-5555-6666-7777	David	**3**	444-4444

INCOME automatically masked by DB2!



Satisfy Your Auditor:
DB2 can now manage different versions of your data

- Application programmers and database administrators have struggled for years with managing different versions of application data.
- New regulatory laws require maintaining historical versions of data for years.
- Every update and delete of data requires applications to copy data to history tables.
- Existing approaches to application level data versioning complicate table design, add complexity and are error prone for applications.



New Temporal table

- New Temporal table allows DB2 to automatically maintain different versions of your data
- Two types of time sequences of table rows are supported through the introduction of database defined time periods
  - SYSTEM_TIME is used to support data “versioning” which archives old rows into a history table
  - BUSINESS_TIME is a period that represents when a row is valid to the user or application
  - BITEMPORAL table combines SYSTEM_TIME period and BUSINESS_TIME period

Defining system period on an existing table

- System versioning is implemented by altering an existing or creating a table with two timestamps, a history table, and defining the versioning relationship between tables
- After the base and history tables are appropriately defined:
  - ALTER TABLE table-name ADD VERSIONING is specified on the base table that is to be versioned
- Auditor can query historical data through SQL
  - DB2 rewrites the user’s query to include data from the history table

DB2 10 for z/OS Security Enhancements

Help Satisfy Your Auditors using new features

- ✓ New granular authorities to reduce data exposure for administrators
- ✓ New auditing features using new audit policies comply with new laws
- ✓ New row and column access table controls to safe guard your data
- ✓ New temporal data to comply with regulations to maintain historical data

References

- DB2 10 for z/OS Technical Overview (SG24-7892-00) available at

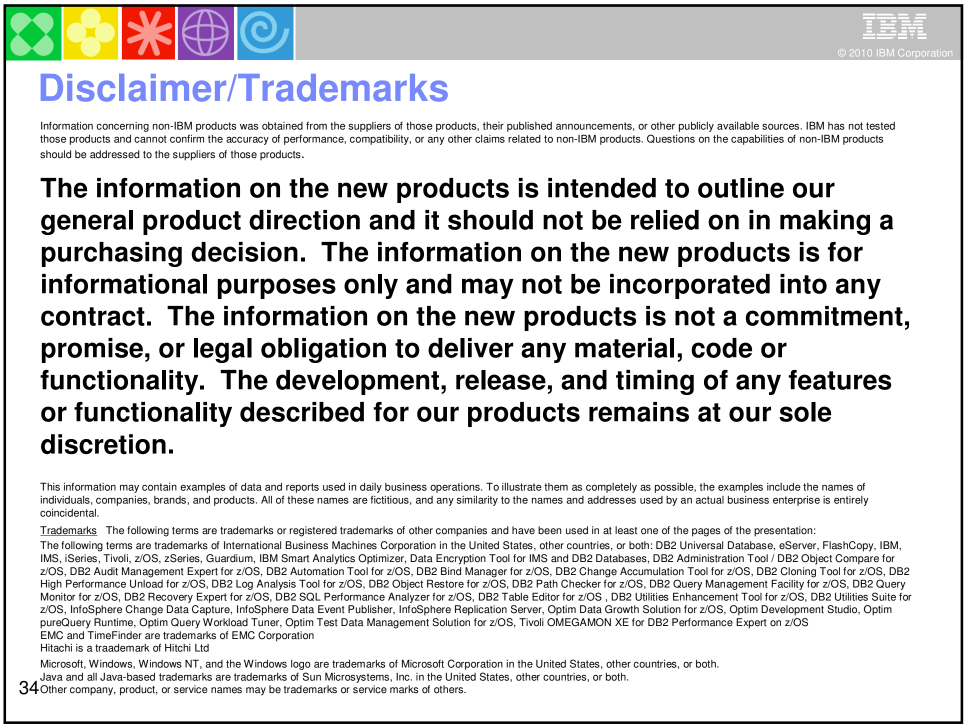
  http://www.redbooks.ibm.com
- DB2 10 for z/OS Administration Guide (SC19-2968-02)

  http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z10.doc.admin/src/admin/db2z_admin.htm
- DB2 10 for z/OS RACF Access Control Module Guide (SC19-2982-02)

  http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z10.doc.racf/src/racf/db2z_racf.htm
- DB2 V10: A new standard in data protection, by Mark Nelson, Randy Love, Gayathiri Chandran, zJournal, February 2011 available at

  http://publibz.boulder.ibm.com/zoslib/pdf/EOZ2N1C0.pdf
- DB2 for z/OS Information Center

  http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp



Disclaimer/Trademarks

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The information on the new products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information on the new products is for informational purposes only and may not be incorporated into any contract. The information on the new products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious, and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks   The following terms are trademarks or registered trademarks of other companies and have been used in at least one of the pages of the presentation:

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both: DB2 Universal Database, eServer, FlashCopy, IBM, IMS, iSeries, Tivoli, z/OS, zSeries, Guardium, IBM Smart Analytics Optimizer, Data Encryption Tool for IMS and DB2 Databases, DB2 Administration Tool / DB2 Object Compare for z/OS, DB2 Audit Management Expert for z/OS, DB2 Automation Tool for z/OS, DB2 Bind Manager for z/OS, DB2 Change Accumulation Tool for z/OS, DB2 Cloning Tool for z/OS, DB2 High Performance Unload for z/OS, DB2 Log Analysis Tool for z/OS, DB2 Object Restore for z/OS, DB2 Path Checker for z/OS, DB2 Query Management Facility for z/OS, DB2 Query Monitor for z/OS, DB2 Recovery Expert for z/OS, DB2 SQL Performance Analyzer for z/OS, DB2 Table Editor for z/OS , DB2 Utilities Enhancement Tool for z/OS, DB2 Utilities Suite for z/OS, InfoSphere Change Data Capture, InfoSphere Data Event Publisher, InfoSphere Replication Server, Optim Data Growth Solution for z/OS, Optim Development Studio, Optim pureQuery Runtime, Optim Query Workload Tuner, Optim Test Data Management Solution for z/OS, Tivoli OMEGAMON XE for DB2 Performance Expert on z/OS
EMC and TimeFinder are trademarks of EMC Corporation
Hitachi is a traademark of Hitchi Ltd

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Other company, product, or service names may be trademarks or service marks of others.