Audit approach of DB2 on mainframe

GSE DB2
09/06/2011

Jean Van Espen
internal audit KBC

Agenda

- Audit steps
- Audit objective
- Inherent risks
- Possible or expected controles
  - Availability
  - Integrity
  - Confidentiality

Audit steps

- Audit assignment (objective, scope, budget)
- List inherent risks and possible or expected controls
- Interviews, reading documents, guides
- Execution of tests
- Evaluation of controls → residual risks
- Audit report with issues
  - Auditee management can agree (= make action plan), disagree or take the risk
- Follow up

Objective

- The objective is to evaluate whether the risks related to the use of DB2 database systems are sufficiently managed. This includes the risks linked to operations, performance and capacity management, systems security and management of support activities.

- Even an audit as a limited time and money budget

Risks (1/3)

- System failures are not timely or proactively detected leading to frequent and long business application outages.
  → availability
- Business data could be wrongly processed, leading directly to incorrect data and unavailability and indirectly to financial losses and other business impacts.
  → integrity

Risks (2/3)

- The data in the databases is insufficiently secured leading to:
  - Fraud potential for internal and external attackers
  - Deliberate acts and errors against integrity and availability of the data
  - Information leakage
  - Unavailability of business applications and integrity problems
  - Unintentional and wrong data processing
- → confidentiality

Risks (3/3)

- Lack of proper segregation of duties between different professional roles leads to:
  - Fraud potential
  - Deliberate acts and errors against integrity and availability of the data
  - Information leakage
  - Unintentional and wrong data processing
- → confidentiality

Expected controles → availability

- A preventive maintenance plan for all critical hardware.
  Procedures exist and are applied for installation of patches and new releases.
- Availability, capacity- and performance monitoring.
- Redundant set-up of infrastructure.

Expected controles → integrity (1/5)

- Operator manuals and procedures are in place, clear and up-to-date.
  Procedures for support actions and incident solving are in place and up-to-date.
- Sufficient level of loose coupling of data
  → keep it simple and documented
- New system software and tool releases are analysed and changes are well prepared.
  Configuration parameters are determined and documented.

Expected controles → integrity (2/5)

- Back-ups are complete and protected.
  Usability is regularly tested.
- Periodic and ad hoc processing is scheduled and followed up. Alerts, depending on the priority, are generated to warn the operation team. Contact persons are known and within reach in case of further escalation.
  Operation logs are checked to ensure correctness and completeness of processing.

Expected controles → integrity (3/5)

- Educated staff
  - All staff, involved in operation and support actions for the DBMS, has sufficient expertise.
  - Back-up staff with sufficient expertise is available for all critical processing.
  - Criticality and confidentiality of the databases is known by the staff.

Expected controles → integrity (4/5)

- Robust application architecture
  - Sufficient measures are taken to guarantee consistent data when one application has to make data changes at several database systems simultaneously.

Expected controles → integrity (5/5)

- Change management
  - Changes to database definitions are executed during planned windows. Users are warned in advance about the foreseen unavailability.
  - All changes to database definitions are clearly documented and sufficiently tested in analogous test environments. Taking backups and checkpoints and fall-back scenarios are elaborated in advance.
  - All changes to database definitions are executed by a dedicated team. Other persons do not have the authorisation to execute the changes.

Expected controles → confidentiality (1/6)

- Security baseline: apply or explain
  - Installation and parameter settings
  - Enforcing the consultation of the security system for each database access
  - Definition of authorised interfaces to the databases
  - Definition and documentation of the purposes for system exits
  - Definition and management of internal security (= roles, authorisations and user access)
  - Secure access to the data by applications
  - Secure access to the data by software tools
  - Secure use of data administration utilities

Tests Security Baseline(1/2)

- Review of installation parameters by looking to the installation JCL's and to the current values by using Mainview.
  Change management of parameters.
- Check (within RACF) that RACF is activated as security system for DB2 access
- Management of exits
- Baseline for access granting to plans for applications using static SQL

Tests Security Baseline (2/2)

- Baseline for access granting on individual tables and views (→ use of dynamic SQL)
  - Update authority of all tables, managed by applications, has to be very limited
  - Read authority of all tables and views managed by operational applications has to be very limited
  - Limit access of functional users to specific tables
    - → need to document purpose of functional users
    - → trust on other audits about infrastructure on systems allowing distributed access to DB2

Expected controles → confidentiality (2/6)

- Review of the security configuration occurs at regular times.
- Access from remote servers and workstations is described and adequately secured.
  Network interfaces are protected from unauthorised access to the data or to the configuration of the databases.
- Security incidents are detected, assessed, documented, reported and acted upon in time.

Expected controles → confidentiality (3/6)

- Programs, running online or in batch on production databases, are protected from unauthorised access and under control of ICT Operations staff.
- Mass exports from production databases are under control of ICT Operations staff. The exported files are appropriately secured.
- Third party access to databases is managed and based on contractual agreements.

Tests on execution of static SQL (1/2)

- Rule in KBC: all in-house development on operational tables uses static SQL and plans with collection list(s)
  → check bind and bindagent authority
  → check execute ability
  1 insecured plan undermines all access control

Tests on execution of static SQL (2/2)

- SELECT PLANNAME FROM SYSIBM.SYSPACKLIST WHERE COLLID = ‘xxxxxxx'
- SELECT A.NAME, A.SYSTEM, B.GRANTEE, B.EXECUTEAUTH FROM SYSIBM.SYSPLSYSTEM A, SYSIBM.SYSPLANAUTH B WHERE A.ENABLE = 'Y' AND A.NAME = B.NAME

Expected controles → confidentiality (4/6)

- Logical Access Management
  - Requests for access rights are formally approved before they are granted on a need to have base.
  - Every user has a unique identifier (UserID) for his personal and sole use and vice versa.
    → shared or technical or functional UserID: need for additional controls
  - Job change → access rights disabled within 30 days
  - User ids and access rights of users, who have left the organisation, are disabled immediately

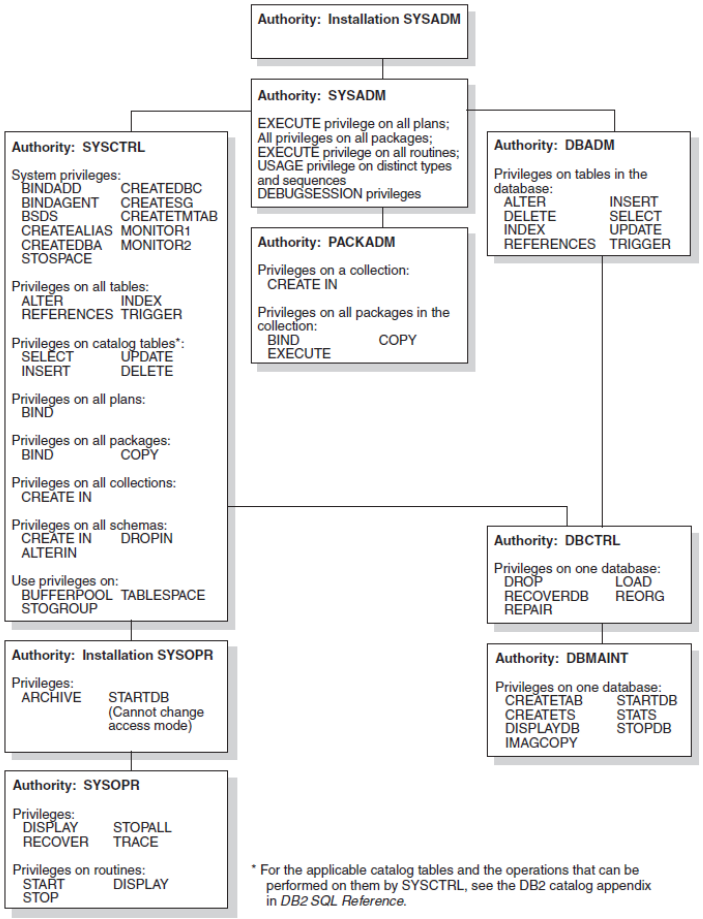
Expected controles → confidentiality (5/6)

- Computer audit logging
  - Owners are defined for the business package. Audit logging requirements, design and implementation are documented.
  - Auditable events both on system level and on application level have been specified; audit records include sufficient information to create accountability (what, when, where & who).
  - Audit logs are protected against unauthorised access and retained for a sufficient timeframe
  - Collection, monitoring and review of audit logs is defined and established.

Expected controles → confidentiality (6/6)

- The segregation of duties principle is honoured between all relevant professional roles.
  - Users
  - Developers
  - Database administration support
  - Database system support
  - Database operational tasks

Roles: see IBM DB2 Admin guide



Check roles in catalog

- SELECT GRANTEE, SYSADMAUTH, SYSOPRAUTH, SYSCTRLAUTH, CREATEDBAAUTH, BINDADDAUTH, STOPALLAUTH, TRACEAUTH, BINDAGENTAUTH FROM SYSIBM.SYSUSERAUTH WHERE SYSADMAUTH > ' ' OR SYSOPRAUTH > ' ' OR SYSCTRLAUTH > ' ' OR CREATEDBAAUTH > ' ' OR BINDADDAUTH > ' ' OR STOPALLAUTH > ' ' OR TRACEAUTH > ' ' OR BINDAGENTAUTH > ' '


KBC