Craig S. Mullins

Return to Home Page

February / March 2009

zData Perspectives

by Craig S. Mullins

Recovery Is A Compliance Issue

When data professionals think about regulatory compliance we tend to consider only data in our production databases. After all, it is this data that runs our business and that must be protected. So we work to implement database auditing to know who did what to which data when; or we tackle database security and data protection initiatives to protect our data from prying eyes; or we focus on improving data quality to ensure the accuracy of our processes.

These are all worthwhile endeavors, but focusing exclusively on active, production data is insufficient to ensure compliance. Improved backup and recovery practices and procedures must be an essential component of your compliance plans.

Ensuring the integrity and availability of your databases is the primary focus of backup and recovery planning. Indeed, as I have written here before, recoverability must be the **primary** objective of every DBA – not performance,

as some assume. After all, it should be easy to achieve fast performance to inaccurate (or worse, non-existent) data, right?

But what about compliance and regulations? Let's examine database recovery through the lens of COBIT.

COBIT is a framework of IT best practices that companies can use to improve management over their IT organizations, to improve the value of IT, and to ensure that the goals of the IT organization are aligned with the goals of the business. COBIT is about recognizing and safeguarding the value of information as a corporate asset by identifying and managing risks and ensuring corporate governance via effective controls. The crux of COBIT is to link IT and business goals, identify responsibilities of business and IT owners, and to monitor performance, evaluating it against metrics and maturity models.

The COBIT framework consists of 34 specific control objectives, organized into 4 domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). The COBIT practices are business focused, process oriented, measurement driven, and control based. Best practice frameworks like COBIT are vital tools for ensuring compliance with regulations such as Sarbanes-Oxley (SOX).

COBIT and Recovery

Database recovery needs to be tackled from a best practice approach to enable your organization to do the kind of up-front planning and routine monitoring and evaluation that COBIT advocates. An organization that has adopted COBIT as a best practice framework understands the critical value of information to the business, and the need to assure its integrity and availability.

Yes, you must develop backup policies and procedures for all of your database objects that match your business availability requirements. Most DBAs have

done this, at least to some degree. But what most have not done is implement regular systematic checks for the on-going viability of their backup and recovery plans to match their recovery time objectives – or even to ensure that their existing backups are valid and could be used in a recovery situation.

Recoverability is addressed by the following 19 COBIT objectives across 3 process domains:

- PO9.4: *Assess risks* - during planning and organization you must assess the risk of databases being unrecoverable from backups.

- DS1.3 and DS1.4: *Define and manage service levels* - metrics are required to defining service level objectives for recovery. Do you know how long it would take to recover a specific database object (or series of objects)? If not, how can you assure that application service levels will be met or exceeded?

- DS3.2, DS3.3, DS3.4, DS3.5 and DS3.8: *Manage performance and capacity* -
  regularly checking the health of your recovery aids capacity management by improving the availability of information and the IT resources that depend on it.

- DS 4.10, DS4.11, and DS4.12: *Ensure continuous service* – again, ensuring service is impossible without being able to ensure recoverability (including that mirrored to backup IT sites and/or offsite backup data stores).

- DS11.9, DS11.19, DS11.20, DS11.21, DS11.23, and DS11.24: *Manage data* -
  any number of issues may require recoverability as part of an on-going data management effort. COBIT Objective DS11.24 specifically covers verifying

the usability of backups.

- M1.1 and M1.2: Monitor the processes – on-going monitoring of recoverability is needed to verify every backup job and its effectiveness in your environment (logging, memory, system resources, etc.)

Organizations need to better acquire and implement tools and procedures that help to verify the integrity of your backups, the system settings that could affect your ability to recover, and the processes associated with backup and recovery of your databases. Analyzing your database system, data, and backups, and determining their health and usability should be a regular practice. If not undertaken, then a system failure, logical error, malicious destruction, or catastrophic event could render your databases unusable, impact your business, and maybe even threaten the on-going viability of your business.

From zJournal, Feb / Mar 2009

.

Home.