Central Control and Coordination

In a database environment such as Adabas, the same data is used by many applications ("users") in many departments of the organization. Ownership of and responsibility for the data is shared by departments with diverse and often conflicting needs. One task of the DBA is to resolve such differences.

Data security and integrity are no longer bound to a single individual or department, but are inherent in systems such as Adabas; in fact, the DBA controls and customized security profiles offered by such systems usually improve security and integrity.

In the past, application development teams have been largely responsible for designing and maintaining application files, usually for their own convenience. Other applications wishing to use the data had to either accept the original file design or convert the information for their own use. This meant inconsistent data integrity, varied recovery procedures, and questionable privacy safeguards. In addition, little attention was given to overall system efficiency; changes introduced in one system could adversely affect the performance of other systems.

With an integrated and shared database, such a lack of central control would soon lead to chaos. Changes to file structure to benefit one project could adversely influence data needs of other projects. Attempts to improve efficiency of one project could be at the expense of another. The use of different security and recovery procedures would, at best, be difficult to manage and at worst, result in confusion and an unstable, insecure database.

Clearly, proper database management means that central control is needed to ensure adherence to common standards and an installation-wide view of hardware and software needs. This central control is the responsibility of the DBA. For these and other reasons, it is important that the DBA function be set up at the very beginning of the database development cycle.