- **Functions and motivations of DA and DBA roles**
- **Organizational Issues**
- **Data Repository Systems**
- **Control over DA and DBA**

Functions and motivations of DA and DBA:

When management first recognized the need for an independent mediator to resolve data-resource conflicts, their response was to create the database administration role. A single role proved inadequate, however, for two reasons. First, it became clear that competency in the role required two different types of skills: A set of administrative skills was needed to handle managerial and policy matters and to interact effectively with database users, and a set of technical skills was also needed to handle the detailed design work and to tune the database so it could be used efficiently. Few people have both sets of skills. Second, over time, the database administrator's workload became excessive. As the amount of end-user computing, decentralized computing, and distributed computing in organizations grew, substantially more support had to be provided, especially to database users who were not information systems professionals. Consequently, the database administration role was split. A new role was created, the data administration role, to handle administrative and policy matters. The database administrator's role was then redefined to focus on technical matters.

Table 6–1 provides an overview of the functions that Everest (1986) says the DA and the DBA should perform in an organization. In the following sections we examine these functions in more detail and discuss some audit procedures we can use to collect evidence on how well they are performed (see also Weber and Everest 1979). Auditors must have a good understanding of the DA's and DBA's functions for the following reasons:

1. If the DA and DBA do not perform their functions well, asset safeguarding, data integrity, system effectiveness, and system efficiency in a database environment can be severely undermined.
2. The DA and DBA are important sources of information on strengths and weaknesses in a database environment because they are focal points for communications among users of the database.
3. The DA and DBA provide important administrative and technical information auditors need to know to carry out that work. For example, the DA might provide the definition of data the auditor needs to access, and the DBA might assist the auditor to use a database tool to retrieve these data.

TABLE 6–1 Data/Database Administration Responsibilities

Function	*DA Responsibilities*	*DBA Responsibilities*
Defining data	Undertaking strategic data planning; determining user needs; specifying conceptual and external schema (user-oriented) definitions.	Specifying internal schema (computer-oriented) definition.
Creating data	Advising users on data-collection procedures; specifying validation and editing criteria.	Preparing programs to create data; assistance in populating database.
Redefining/ restructuring data	Specifying new conceptual . and external schema definitions; advising users on how to conform with new definition.	Specifying new internal schema definition; altering database to conform with new schema definitions.
Retiring data	Specifying retirement policies.	Implementing retirement policies.

Making database available to users	Determining end-user requirements for database tools; testing and evaluating end-user database tools.	Determining programmer requirements for database tools; determining database optimization tools required; testing and evaluating programmer and database optimization tools.
Informing and servicing users	Answering end-user queries; educating end users; establishing and promulgating high-level policy information; providing conceptual schema and external schema information.	Answering programmer queries; educating programmers; establishing and promulgating low-level policy information; providing internal schema information.
Maintaining database integrity	Developing and promulgating organizationwide standards; assisting end users to formulate application controls.	Implementing database controls; assisting programmers to design and implement application controls.
Monitoring operations	Monitoring end-user patterns of database use.	Monitoring programmer patterns of database use; collecting performance statistics; tuning the database.

Organizational Issues:

The preceding sections adopt a normative perspective of the DA and DBA roles; that is, they discuss what these roles *should* be accomplishing to provide auditors with a basis for evaluating them. Unfortunately, the situation in practice is not as clear-cut as the normative descriptions imply. Both the DA and DBA roles are relatively new, and a number of unresolved difficulties remain. An early study by Kahn (1983), for example, found the DA and DBA roles were only marginally effective, even though they were adequately funded. More recent work by Braithwaite (1988) and Vinden (1990) indicates this situation still persists and is likely to continue for some time.

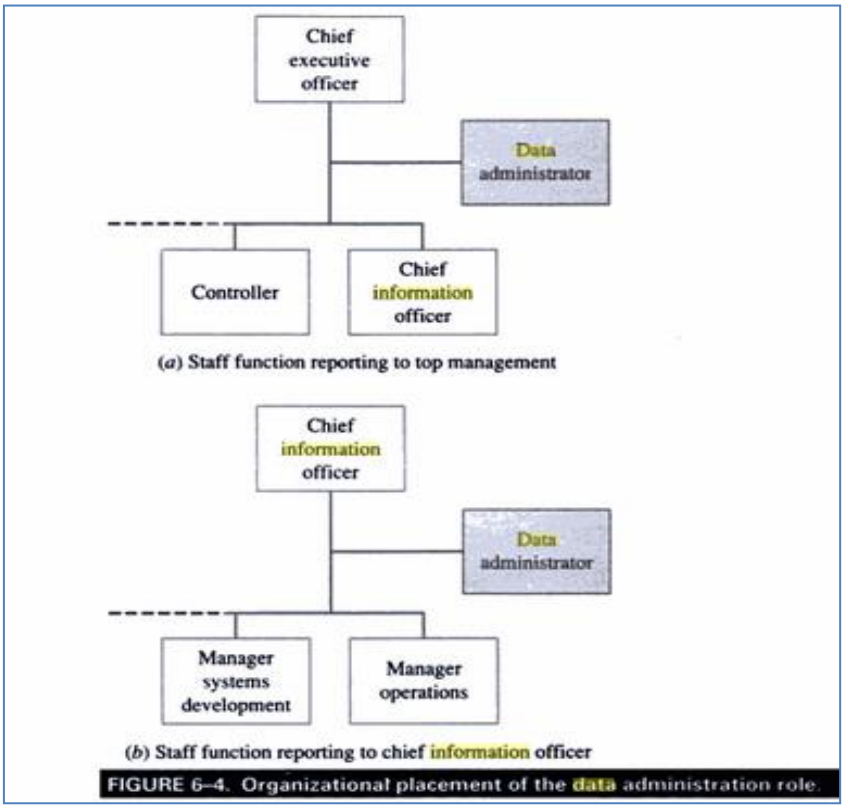
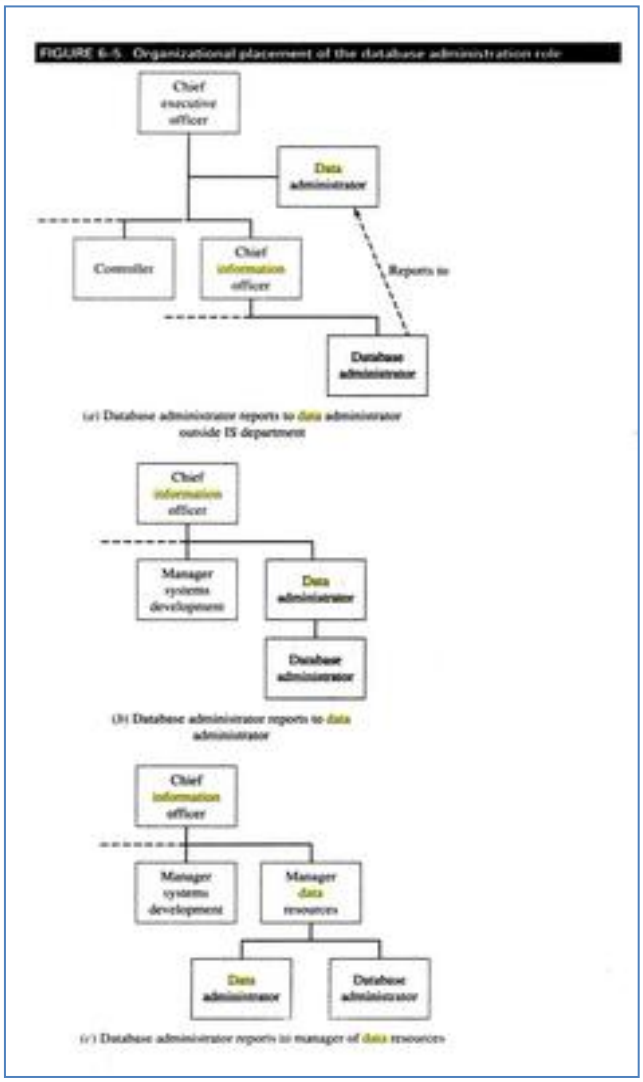


FIGURE 6–4. Organizational placement of the data administration role.

In this light, the following sections examine two major organizational issues that must be addressed if the DA and DBA roles are to be effective: the placement of the DA and DBA roles in the organizational hierarchy and the impact of decentralization of the information systems function on the DA and DBA. We will see these two issues mean that auditors must evaluate both roles from a contingency perspective.

Irrespective of an organization's position within the strategic grid, the DBA seems best placed under the person who controls the information systems function. Because DBAs undertake many technical activities, there are advantages to having them located in close proximity to hardware/software resources and to the information systems staff. Nevertheless, the DBA must work closely with the DA. If the DA role is located in the offices of top management, the DBA must be able to communicate directly with the DA and not be constrained by formal lines of reporting within the organization (Figure 6–5*a*). If the DA role is located in the information systems function, however, the DBA might report directly to the DA (Figure 6–5*b*). In large factory organizations, both the DA and DBA might even report to a manager who takes overall responsibility for the organization's data resources (Figure 6–5*c*).

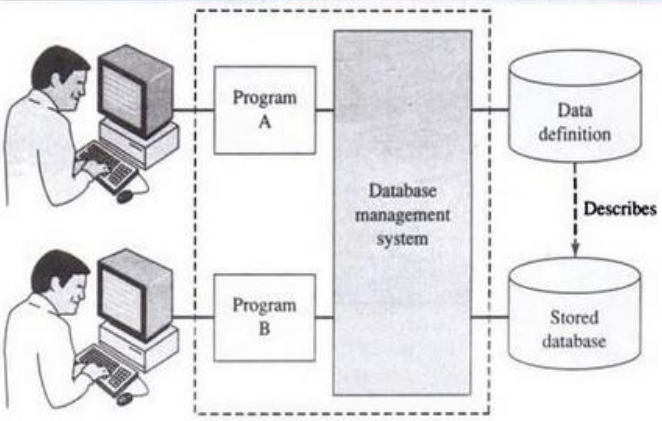
If auditors conclude that the DA and DBA functions are not located appropriately—for example, in a strategic organization they are both located under the manager of systems development—they should assess the risk of ineffective performance of both roles to be higher. As a result, there is a higher risk that the quality of database application systems will be undermined. Accordingly, they will need to expand their detailed testing of these application systems during subsequent stages of the audit.



Data Repository System (DRS):

Recall that two major objectives of database management are to facilitate evolution of the database and to maintain database integrity. These objectives can be accomplished in several ways. A primary means, however, is to maintain a single, complete, automated definition of the data and to separate this definition from the data itself and from the programs that use that data (Figure 6–7). If a single, complete, automated definition is maintained, all users and programs have access to a common, consistent, up-to-date description of the data.

FIGURE 6–7. Using a separate data definition to achieve the objectives of database management.



Moreover, by separating the definition of data from instances of the data, certain types of changes can be made to the definition without affecting the stored data. For example, in some cases a user's view of the data can be altered without modifying the stored data. Similarly, certain types of changes can be made to the definition without affecting the programs that use the data. For example, the internal schema can be changed without having to alter program source code and to recompile programs.

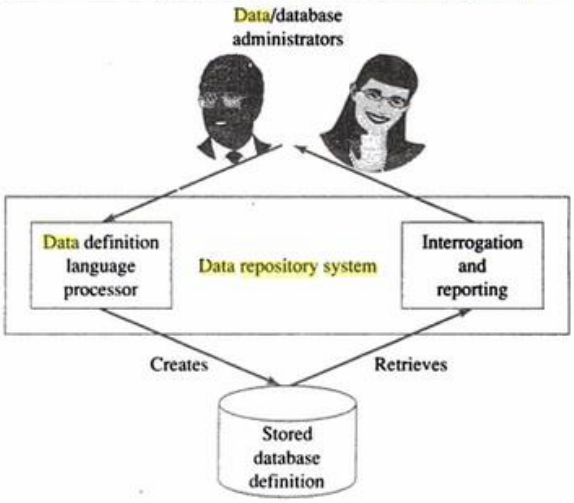
The facility used to maintain an automated definition of the data is called a data dictionary system, data directory system, or more recently a data repository system (DRS). Auditors must be familiar with the nature and functions of a DRS and its importance for the audit conducted. In this light, the following three sections review the basic functions of a DRS, some problems with DRSs that can undermine controls, and the relevance of DRSs for the auditor's work.

Basic Functions of a DRS

As discussed previously, the primary function of a DRS is to store the database definition. Recall that three types of definition are required to provide a complete description of the database: a conceptual schema definition, an external schema definition, and an internal schema definition. Because these definitions are data themselves, they are sometimes called "metadata"; they are data about data. This metadata should provide an authentic, accurate, complete, consistent, and up-to-date description of the database that can be employed by *(1)* programs that must access and manipulate the database and *(2)* users who must carry out their day-to-day activities as well as plan and provide for their future activities.

To support these needs, Figure 6–8 shows the major functional capabilities that a DRS must provide. A data definition language processor allows the DA/DBA to create or modify a data definition. It performs validation tests on the definition entered by the DA/DBA to ensure the integrity of the metadata

FIGURE 6–8. Major facilities in a data repository system.

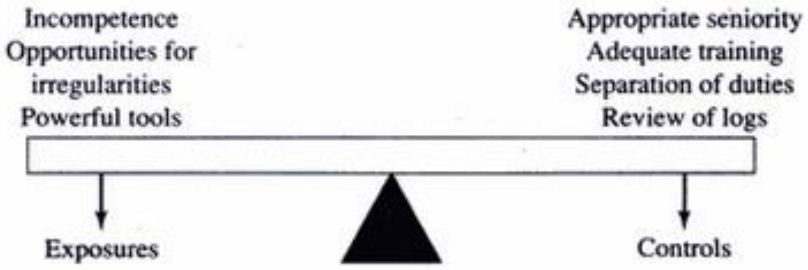


Control Over DA and DBA:

Even a cursory examination of the functions performed by the DA and DBA shows that substantial power can be vested in these roles, particularly in turnaround and strategic organizations in which information systems are critical to the organization's success. This power can be used with propriety; alternatively, it can be abused. On the one hand, centralizing certain functions to be performed in a database environment improves communication, coordination, and control. On the other hand, vesting substantial power in the DA and DBA roles runs contrary to fundamental principles of sound internal control.

Auditors must understand how the powers vested in the DA and DBA roles can be used to undermine control. They must understand, also, how the exposures that arise can be reduced. In this light, the following sections briefly examine the nature of the exposures and some remedial measures that can be used to reduce expected losses from these exposures (Figure 6–11).

FIGURE 6–11. Control over data administration/database administration exposures.



Three types of exposure arise by virtue of the nature of and existence of the DA and DBA roles:

1. *Incompetent performance of roles:* In some organizations (e.g., strategic organizations), the functions performed by the DA and DBA can be complex and demanding. For example, the DA must be a visionary to foresee long-term data needs and an astute diplomat to perform mediation functions effectively. The DBA must excel technically if the database is to be used efficiently and the inevitable user conflicts are to be mitigated. Because the DA and DBA play pivotal roles in a database environment, poor performance by the incumbents can quickly undermine asset safeguarding, data integrity, system effectiveness, and system efficiency objectives.
2. *Opportunities to perpetrate irregularities:* On the one hand, centralization of power in the DA and DBA roles simplifies complex communication and coordination functions that must be performed in a database environment. On the other hand, it provides opportunities to perpetrate irregularities. The powers vested in the DA and DBA might violate the fundamental internal control principle of separation of duties. For example, the DA might have the power to authorize user access privileges and to set up these privileges in the DBMS via the access control mechanism. Thus, the DA both authorizes and executes the activity. If no one subsequently checks the DA's work, improper access privileges could be granted to a user such that irregularities can then be perpetrated.
3. *Availability of tools to override controls:* Both the DA and DBA have available powerful tools that they need to establish and monitor controls in a database environment. For example, they can set up various levels of access and update authorizations, perhaps find out user passwords, and possibly gain access to and change audit trails and log files. Improper use of these tools can undermine asset safeguarding and data integrity objectives. For example, the DA or DBA might increase funds in a friend's bank account and then alter the audit trail to remove any trace of the unauthorized activity.

If only a DBA position exists in an organization, these exposures become more salient. The DBA's work will not be monitored by a DA. Consequently, there are more opportunities for improprieties and undetected errors. Even if a DA position exists, however, auditors must be alert to the possibility of collusion between the DA and the DBA.

* * * * * *