

## Harvard University General Policies & Procedures

Title:	Data Warehouse Security
Area:	Reports
Process:	Ad-Hoc Querying
Policy Issue Date:	6/10/99

### University Policy Overview:

Ad-hoc use of the Harvard Data Warehouse (HDW) is secured by two mechanisms: rules controlling access to Chart of Accounts (CoA) values and flags controlling access to specialized data areas. Both the CoA rules and the flags are attached to Oracle responsibilities, and users are assigned one or more responsibilities. Security administrators within each tub determine which responsibilities each of their staff has. Security administrators within Financial Administration determine which staff have university-wide access, that is, no CoA rules in their responsibilities.

The CoA rules govern row-level access, determining exactly which rows within a table a person is allowed to see. The flags, on the other hand, govern access to whole tables, determining whether a person is allowed to see the tables at all.

Some data warehouse reference tables, for example, the list of tub values, are unsecured. Other tables, such as those containing General Ledger transactions, are secured only by CoA rules. Yet other tables, such as those which list the security rules, are controlled only by a flag. Finally, there are tables such as expense report entries from STAR, which are controlled by both CoA rules and a flag. The data model displays information about the security status of each table in the HDW.

### People with Multiple Responsibilities

Security administrators may give people more than one responsibility. Such individuals see all the data to which any of their responsibilities entitle them.

#### Example:

**Judy Sikhtia has two reporting responsibilities. The first lets her see the transactions for a mega-org having object codes for income, expenses, and balances forward. This responsibility has a flag permitting access to STAR detail. The second lets her see all of the transactions for a range of sponsored activity values. This responsibility has flags permitting access to STAR detail, HURIS data, and payroll detail. When she logs on with InfoMaker, Judy can see all transactions for the mega-org and the permitted object values, and also all transactions for the sponsored activities with any object value. Because her second responsibility gives her access to the HURIS data and payroll detail, she can see payroll detail for the mega-org and HURIS data for any sponsored activities used with that mega-org.**



---

## Recommended Method for Defining Responsibilities

Project ADAPT provided instructions to security administrators for defining initial reporting responsibilities. The instructions recommended that people choose one of about ten security rules on the object segment, and then a security rule on a single other segment (tub, org, fund, activity, or root). The instructions pointed out that cross-validation rules would prevent many segment values from being used together and that it was therefore not necessary to replicate the cross-validation rules in the security rules. For example, a person with a security rule on org would not need a security rule on tub, because a given org value may be used only with one tub. In a few cases, responsibilities have more complex combinations of CoA rules, governing access to more than two segments.

