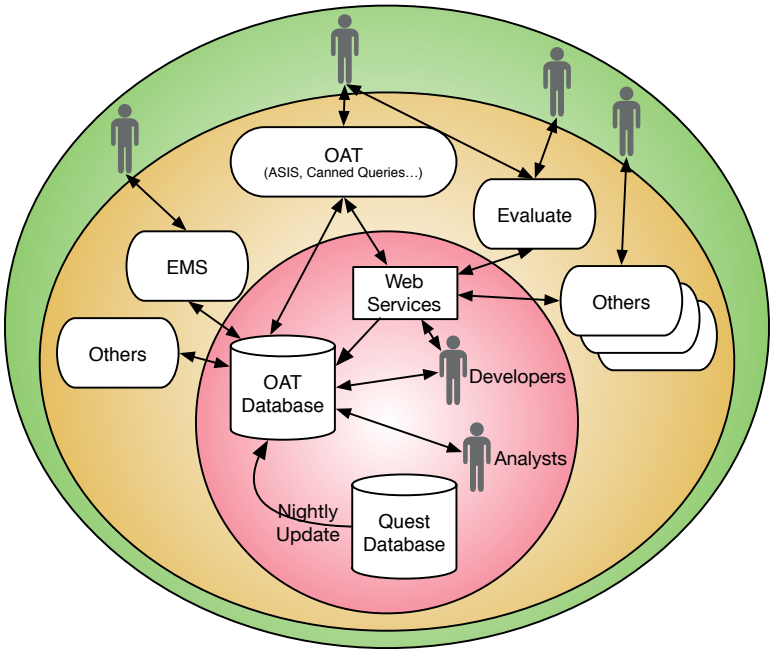
Access to the OAT Database

This document describes how the OAT database may be accessed, including access by people ("users") and by applications.

The following diagram shows the high-level architecture. The OAT Database is the central resource of concern in this document. It is updated nightly from the Quest database. The OAT Database may be accessed via SQL or web services, either by people or programs. People may access it directly (via SQL or web services) or indirectly (via an application program).



Definitions:

1. OAT database: The database that stores data from Quest and other sources and is the central subject of this document. In some contexts this database is also known as "Odyssey".
2. Application: A program that accesses data from the OAT database. Current examples include the OAT suite of tools (ASIS, canned queries, etc), the Exam Management System, and Evaluate.
3. Application users: People who access the OAT database indirectly through an application. This is by far the most common case.
4. Analysts: People who have the SQL skill and appropriate permissions to write queries against the OAT database to:
    a. answer immediate one-off questions for administrative and/or academic support,
    b. create repeat-use queries to be added to OAT's collection of canned queries,
    c. or, create single-user applications using tools such as Excel, Access, or R.
5. Developers: People who develop applications that depend on OAT data and will be accessible to other users.

Core Principles

Core Principles for Application Users

1. Access to confidential data, including the data stored in the OAT database, is governed by University Policy 46. This document clarifies how Policy 46 is implemented with respect to the OAT database. If any conflict arises, Policy 46 takes precedence.
2. Anyone who is given access to data via OAT is bound by Policy 46 and Appendix A (Access to and Release of Student Information) in particular.
3. Some applications allow data to be downloaded to local machines. Users will not store such data longer than necessary to complete the immediate business function.

Core Principles for Analysts and Developers

1. **Don't store data.**
2. Analysts will endeavour to write their queries to be applicable to as broad an audience as possible and will submit appropriate queries to be included in OATs Canned Queries feature.
3. Developers will give appropriate consideration to making their applications available to other UWaterloo users who have similar needs.

Core Principles for Applications

1. Applications will not store data from the OAT database without prior written authorization from the OAT Management Board. Whenever feasible, it is preferable to query OAT again rather than storing data locally.
2. Applications must implement appropriate user access controls.
3. Applications and their sponsors will expect and encourage the above principles for their own users.
4. Each application should have its own approval process and OAT credentials for accessing data.

Gaining Access

Access for Users

Application users gain access by being authorized to use one or more applications via the policies and procedures associated with the specific application.

For example, access to the OAT applications is approved by an Associate Dean, Undergrad, or the equivalent within non-academic units (the "sponsor"). Most users gain access by requesting it from their sponsor. The sponsor has access to a OAT web page that can grant the user specific permissions for using the system. The sponsor may also record a rationale for granting access in case the rationale is not apparent from the user's job title. In some cases, a user may gain access by making a request directly to the OAT Management Board, but such a user still requires a sponsor. Each user account has an expiry date which must be periodically updated by the sponsor or the user will automatically lose access. A second example is the Exam Management System. Access for instructors is automatically granted when they are assigned to teach a course.

Analysts must be nominated by an appropriate authority within their faculty or business unit and be approved by the OAT Management Board ("OMB"). An application to the board should include a brief overview of the query writer's skills, the objectives of accessing the database, and the time-frame for access. Application can be made with an email to the OMB's chair. The OAT Management Board will maintain appropriate records of each request.

Application developers approved by the project's sponsors and the OMB will be given access to at least the same data that the application itself will access. Sometimes developers will be given broader access at the discretion of the project sponsors and the OMB.

Access for Applications

In general, applications should request data from the OAT database when it's needed. They should avoid caching data to disk to avoid many security issues as well as the overhead and complexity of updating stale data.

The technical access mechanisms include:

1. Accessing a web service, either from the set that has already been written or a new one created for the application. This is the preferred approach. It works best when most or all of the data already resides in OAT and does not need to be joined with outside data.
2. If the application needs to store its own data, an application-specific schema could be set up within the same database instance as OAT. It could be used via OAT web services or via direct SQL access.
3. Accessing an application-specific view developed in conjunction with OAT staff. This works best when the application has data that needs to be joined with OAT data at the SQL level and there is already a commitment to an existing database. This assumes that the non-OAT database can access foreign tables. If the data held outside of OAT is generally useful, have a discussion of whether it should be moved into the OAT database.
4. Direct SQL access is also possible with further analysis and approval by the OAT Management Board.

The process for obtaining access:

1. The project sponsor develops a project description. It will describe the project's purpose, users, the data that will be used, and specifically, the data required from OAT and how that data will be accessed.
2. The OMB considers the project description and answers four questions:
    a. Are we able to provide the requested data (e.g. do we have it in our database or can we get it)?
    b. Are we willing to do the work required to provide the data?
    c. Whose approval-in-principle do we require to proceed? This is likely to be some subset of the Registrar, Associate VP for Graduate Studies, a Dean, etc. For public data, the list of required approvals will be empty (where "public data" means that it is already available from a public UW web site; examples include calendar data and course offering data).
    d. Whose approval do we require to put the application into production? This will likely be a subset of the people listed in 2c and probably IST's Information Security Services team.

3. If OAT is willing and able to do the work and after the required permissions are received, we'll work with the project developers to build the required infrastructure in our test system (e.g. with stale data).
4. Upon final approval from the people listed in 2d, we'll move the infrastructure from test to production.
5. As noted earlier, the OMB will not grant permission for a project that stores confidential records obtained from OAT. Such permission may be granted only by the Information Stewards. Developers seeking to create such a persistent database should initiate the process by completing an Information Risk Assessment Intake Form.

The OAT Management Board will maintain documentation for each development project that requests access. The documentation will consist largely of the information mentioned above.

Revisions:
2019-03-27 Approved by OAT Management Board.