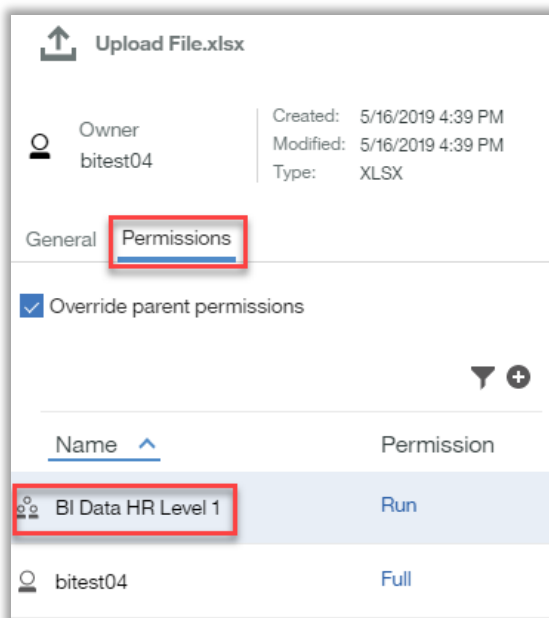
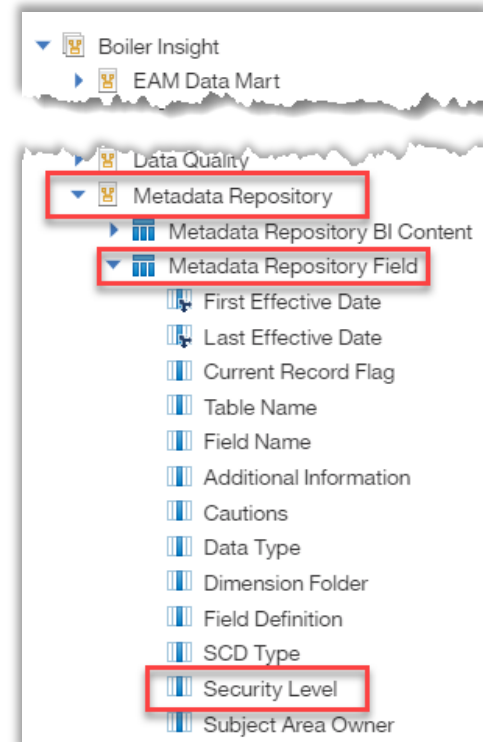


When a report or dashboard is created using the Cognos new features (data set, upload file, and/or data module), the owner of all objects involved, is responsible in ensuring the appropriate security is set in place on those objects. This is especially important when the report or dashboard is in a *Standard Content* folder.

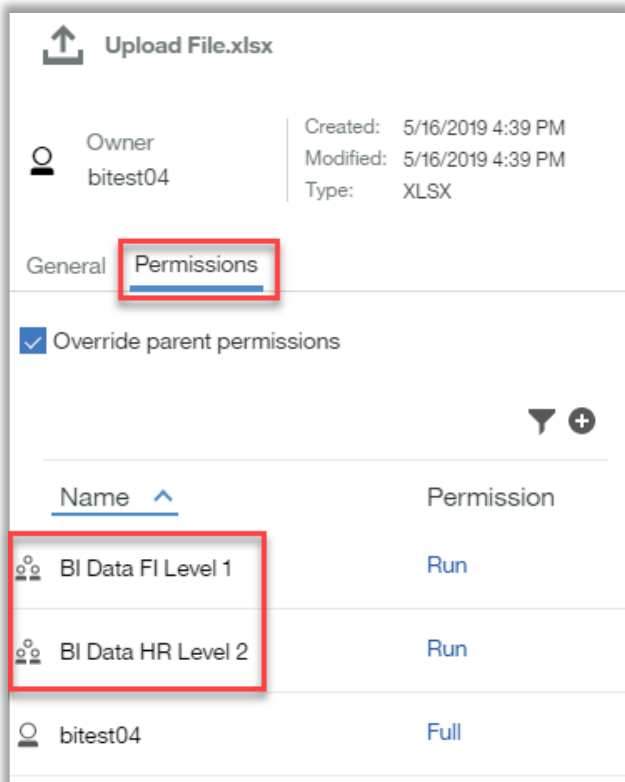
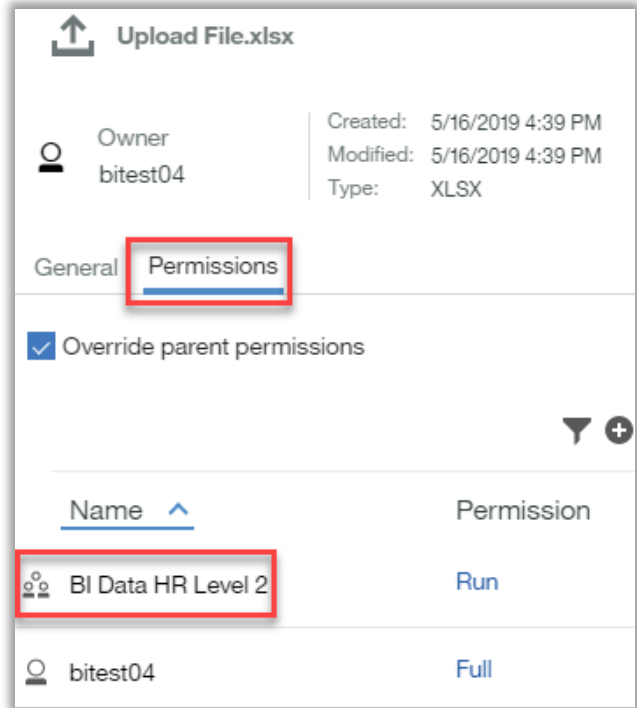
The best practice is to align the security of the data set or upload file with the data fields that are included within it.

If using **Boiler Insight** data - To determine what data role(s) are needed to view the fields within the object (data set or upload file), reference the *Metadata Repository Field* dimension of the *Metadata Repository*. The *Security Level* field provides the role needed to view each field.



For example, this object (upload file) contains HR data that requires the *HR Level 1* role. Therefore, the owner has used the *BI Data HR Level 1* group to secure it.

If the object contains higher secured HR fields that require the *HR Level 2* role, the owner would use the *BI Data HR Level 2* group. *BI Data HR Level 1* would *not* be needed since the roles are hierarchical (If someone has the *HR 2* role, they automatically have the *HR 1* role).



If an object has more than one role permissioned, the intended audience needs to have *all* roles listed to be able to run a report/dashboard that is built with the object. For the example, the audience would need to have both *FI Level 1* and *HR Level 2* to run a report created off of this upload file. Note – You cannot build a report off of an upload file directly, you must put the upload file into a data module and then you can create a report.

If using **Student** data – Fields are secured by access groups. Therefore, what security should be set on the object(s) can be determined by what access groups are needed to view the fields within the object.

**Caution** - All of the objects used to create a report or dashboard (data module and/or dataset and/or upload file) need to be saved in a location that the intended audience has access to. For example, for a report that is built off of a upload file and data module – both the upload file and data module need to be housed in a folder where the intended audience has access. This folder does not need to be the *same* folder where the report is housed, just a folder where the audience has at least *run* access.