

# VO Assessment Template



This is a derivative work based on the [CO Requirements Assessment](#) created by the CManage project team and Internet2 as part of a US National Science Foundation grant effort. This work is covered under the Apache2 license.



## Work in Progress

- ☒ Add a column that explains the purpose of each question
- ☐ Create a glossary of terms
- ☒ Add a question and pointer re: Data Protection Code of Conduct
- ☒ Remove any country-specific language
- ☒ Add links where appropriate (e.g., to XSEDE, eduPerson schema)

Profiling your VO - culture and management (A question for the PI /Researcher /Collaboration Coordinator)	Purpose of the question
Describe the scope of your research and collaborations (e.g., broad with significant outreach; narrow with a focus on a single instrument or data set; open community; closed community).	The scope of a VO has significant implications for the IT infrastructure that will be required to properly support it. A VO that focuses on community outreach may require tools that will allow self-signup and social identity authentication mechanisms, whereas a VO that depends entirely on a single instrument may keep much of their collaboration closed off, leaving public access to a later date or a separate environment entirely.
Describe how the leadership of your VO make decisions (e.g., <i>ad hoc</i> ; steering committee; general consensus; distributed based on topic).	Methods of communication between a VO and Research and Education Network (REN) staff will often vary significantly depending on how decisions are made.
How are new services defined, developed, and promoted to the participants (e.g., email list; newsletter; word of mouth)?	This provides a hint as to the rate people will join or use new services, which in turn has bearing on the capacity required for the systems supporting the environment.
VO community (A question for the PI /Researcher /Collaboration Coordinator)	Purpose of the question
Are there specific key campuses or institutions that need to be taken into account in your collaboration?	Federation (and interfederation) still periodically requires direct discussions between campuses and RENs. Knowing who the target campuses can make the necessary interactions run more efficiently.
Are there any particular instruments or resources that will require electronic access control?	This helps with the understanding of how granular access controls will need to be.
Are there participants outside of the R&E community that need to be taken into account (e.g., commercial entities, citizen scientists)?	Identity federation is far more common within the R&E community than in the commercial world. If there are participants in the VO outside of R&E, then it is likely that either social identities or special provisioning of accounts will need to be used for those participants.

Which key funding agencies involved? Do their requirements impact the nature of your collaboration (e.g., require open participation, require public access to data)?	Different funding agencies often have different requirements with regards to participation and access. For example, some funding agencies will require demographic information to determine minority participation. In other cases, funding agencies may require that all data be open to the public, with no access controls. Alternatively, the data may be required to be public, but only after a certain period of time, or after the formal collaboration has ended. These details inform the REN regarding what kind of account and auditing might be required for the VO.
Does you require that the participants in your collaboration use electronic identities that have been verified by a third party, or is self-asserted identity sufficient?	This question assesses what level of identity assurance may be required by the VO. In some cases, a VO may accept self-asserted identity in most cases, but specific access will require high levels of checking.
For VOs with a presence in the EU, how do you protect personal information or register consent for the sharing of personal information of your participants?	Many VOs are unaware or unconcerned about data protection and privacy of personal information within the VO. Depending on how the information is used, however, there are legal concerns that the VO must be made aware of regarding personal information. Introducing the PI, Researcher, or collaboration coordinator to the <a href="#">Data Protection Code of Conduct</a> is an important step in keeping the VO in proper support of individual privacy.
Describe the variations of size and character of groups within the VO.	Groups can be fairly simple, discrete sets of people, or they can be complex sets that require group math to determine participation. Different group management tools will be more or less applicable depending on where in that continuum of group complexity a VO resides.
<b>Use cases (A question for the PI/Researcher /Collaboration Coordinator)</b>	<b>Purpose of the question</b>
Describe one or two "typical" users and their expected activities and interactions with the online collaboration environment.	It is often easier to understand the needs and usage patterns of a VO by walking through specific use cases. For example, a typical use case might involve graduate students who are expected to be enrolled in a particular way and who will need access to specific material. Another use case might involve staff participation, with senior staff requiring greater control over access management.
<b>Users, guests, and contributors (A question for the Collaboration Coordinator/Site Administrator)</b>	<b>Purpose of the question</b>
Who decides what services are given to whom, and when are those services provisioned/de-provisioned?	Some organizations are very top-down driven, with the lead researcher controlling all access. In other organizations, the model is much more open, with individuals able to select their own groups and through that, all associated access. Understanding where along that continuum of control through self-management makes a difference when it comes to planning for a support model.
What roles do people play within your VO? How consistent are the roles (e. g., researcher, data administrator, assistant, guest) across the VO, or do roles often blend?	In an organized world, roles are clearly defined and access can be assigned based on role with no need for overlap. And some organizations do follow that model to the best of their abilities. However, other organizations find themselves in a much more fluid environment, which in turn has impact on the complexity of the support model for the organization.
Who needs to be able to add people? Who is responsible for disambiguation within the registry?	Often, there is no one person responsible for adding individuals or dealing with duplicate entries. This results in unnecessary entries in the directory and confusing access control issues for the user. Making sure that someone at least handles the disambiguation within the Registry is an important support action.
For each of the different types of people joining your VO, what is the invitation model? How are they added /invited/enrolled?	Are individuals sent invitations to join, or are they added by an administrator? Or is there a self-signup form for anyone to use? Making this clear helps the support teams understand the types of questions they may receive from users.
How do you handle changes in affiliation (i.e., a postdoc at institution A becomes a faculty member at institution B, but expects to remain involved in the VO)?	Some VOs require the individual to re-enroll and rejoin the appropriate groups. Others encourage individuals to join with a social identity that will not change through changes in affiliation or organization. Knowing which model the VO follows helps target and configure the support tools appropriately.

What are your reporting requirements around the users in the VO (e.g., real-time or batch reports for new users, staff effort towards research for the VO)?	The VO may or may not have audit requirements from their funding agency. The support staff need to know about such requirements early on in order to ask the correct questions at time of enrollment and to provide the most accurate audit data possible.
<b>Application requirements (A question for the Collaboration Coordinator/Site Administrator)</b>	<b>Purpose of the question</b>
What applications does your VO currently use (e.g., SSH, Sympa or Mailman, Docuwiki or Confluence)? What applications (or types of applications) do you intend to use in the future?	Some applications are easy to integrate into a collaboration platform because they easily accept external authentication and attributes. Others are not nearly as simple. Knowing what tools are required for the collaboration helps prioritize the work to get a collaboration established.
How do people find out about new applications available to your VO?	Does your VO expect a portal to show them what tools are available for them to choose from? Is there a newsletter that informs participants of what tools are available? Setting this expectation early will inform what collaboration platform may be most suited to this environment.
Is single sign-on (SSO) required through the applications in use? If so, are you using a certificate or key based service? How are the certificates or keys managed?	This again will establish what tools are required in a collaboration platform. If your VO uses tools that require X.509 certificates (e.g., <a href="#">XSEDE</a> , <a href="#">Globus</a> ) that will suggest specific support options such as the use of <a href="#">CILogon</a> for your environment.
Will data sets be stored or shared within the collaboration infrastructure?	Some VOs handle the actual science data separately from the collaboration itself. Understanding the data storage and access requirements is critical in establishing the overarching technical architecture for a VO.
Do you have a need for multiple authentication models? If so, describe the models you expect and any other unique factors expressed or implied by having different models available.	There are a variety of use cases possible with regards to authentication. Some VOs, such as the ones that focus on citizen science, rely largely on social identities and use Google or Facebook for their authentication service. Other VOs run their authentication entirely in house, or require that all accounts authenticate through federated higher education institutions. And other VOs may mix and match, requiring different types of authentication (social or vetted educational identities) depending on what material within the collaboration is being accessed. This question opens up some important characteristics that a support team will need to know as they establish or take over management of the VO collaboration infrastructure.
<b>Access control (A question for the Collaboration Coordinator/Site Administrator)</b>	<b>Purpose of the question</b>
Which online resources need access controls (e.g., data set restrictions; domain app restrictions)?	Different applications require different handling when it comes to accepting external authorization and/or group information. By identifying what applications or resources require access control, the support team can start to determine what actions need to be taken to support the VO's environment.
Do you use user profiles to help match users to data sets, permissions, etc.? If so, who defines these profiles, and who (users, admins, systems, etc.) populates them with attributes ?	This is not a usual case, but some VOs, particularly fully open ones, may want to explore matching up types of users with appropriate datasets and applications. Profile information for these users may be available through services such as <a href="#">VIVO</a> , <a href="#">ResearchGate</a> , or <a href="#">Google Scholar</a> . If this is a desired feature, then the support team needs to know about it.
Who determines which resources need protecting?	Permissions may be controlled at the PI level or at the group or team lead level (or whatever the equivalents are within a particular VO). Depending on the model followed, the organizational and group structure needs to be developed around this requirement.
<b>Existing middleware infrastructure (A question for the Site Administrator)</b>	<b>Purpose of the question</b>

Describe your current identity management and authentication models. How does this differ from your ongoing plans or expectations?	It is quite useful for the support team to understand what is already in place for identity management within a VO. It might be spreadsheets and manual account creation. It might be purely social identity logins.
Are there specific schema (e. g., <a href="#">eduPerson</a> , <a href="#">SCHAC</a> , <a href="#">inet OrgPerson</a> ) that are required by your VO?	If the answer here is "I don't know" that is fine. If the VO wants to take advantage of federated access, then <a href="#">eduPerson</a> at the least will be a necessary schema to be ready to support.
<b>Internal IT capabilities (A question for the Site Administrator)</b>	<b>Purpose of the question</b>
List the compute and data platforms (software) currently in use.	A complete list of the tools that will need support, even if it is just identity management support, is critical to being able to scope the level of effort required to support a VO.
List the collaboration platforms, if any, currently in use.	Is the VO using something like Perun, COnanage, or another platform to help manage their environment? Are they moving away from it, or asking another organization to take over management?
Describe if/how your VO uses <a href="#">Google Apps</a> or other outsourced collaboration environments like <a href="#">XSEDE</a> or <a href="#">OSG</a> ..	If the primary collaboration software used by a VO is the Google Apps suite, that will tell a support group that social identity is expected, and will suggest some technical details around what protocols need to be supported (OpenID vs SAML). Depending on the answers to some of the other questions above, there may be some complications here if the VO wants functionality in terms of groups and permissions not supported by a third-party platform.