Policies and controls (Founding company, Foundation and DAO Service Providers)

Control	Description
Internal policies and employee controls	The project should have internal controls agreed to by all employees, including: - Acceptable use policy - Employee device security policy - Password policy including MFA requirements Here is a list of recommended policies.
Identity and access management	The project is recommended to utilize a central identity management system. Examples: GitHub SSO, Azure AD, Okta, Auth0, Cognito, etc… There should be strict internal policies and processes for granting and removing permissions and role memberships. This would include the employee on-boarding (granting access), off-boarding (removing access), and modifying (granting additional access). At a minimum, the project must have a defined and followed employee on/off boarding process.
Vulnerability management	The project should define requirements and enforce controls related to the dependencies and vulnerabilities it imposes on the DAO/ the protocol it serves, as well as their remediations. Sufficient controls include attempting to implement and follow a well known framework such as the OWASP Vulnerability Management Guide.
Data classification	If the project stores or manages user data, the project should have a series of internal controls for: - Classifying the data - Anonymizing the data (IP addresses, PII, etc…) - Segmenting from non-production environments or authorized users - Encryption in transit and at rest or in motion

	● Least privileged access ● Audit logging All employees in the project should be trained to follow appropriate data-handling processes and controls.
Privacy policy	The project provide a basic privacy policy
GDPR (if applicable)	If the project is subject to GDPR, appropriate controls should be in place.
Change Management	The project is recommended to implement change management controls, including: ● Source control (git, etc…) ● Ticketing systems ● Code/change management reviews ● Agree to change management policy if needed ● Usage of configuration management tools
Incident reporting	The project and the DAO should agree prior on what defines an incident, how they will be identified and reported.
Disaster Recovery	The project must have a well defined disaster recovery policy and annual review/simulation. Objectives to consider: ● RPO and RTO (Recovery Point Objective) and (Recovery Time Objective) ● Technical assets governed by the DR policy should be universally agreed upon by all stakeholders. ● Well defined failover and recovery plans. ● Communications and community status updates. ● Wargamed exercises i.e. foundation controlled sequencers become unavailable due to a multi-cloud outage. How is recovery handled? Example template.
Data retention	The project is advised to define and implement retention policies for data, including: ● Log retention ● Email ● Documents ● Jurisdictional or regulatory retention

	requirements for applicable data Application logs should be regularly reviewed for information or data leakage. There should be appropriate backup processes in place and access controls relating to retained data.