Enterprise Neurosystem ML Governance

Proposed Staged Governance Model, Mar 7, 2022
Audrey Reznik, Erik Erlandson, Lisa Caywood

Why use ML Governance?

What is ML Governance?
ML governance is the **process of defining policies and establishing accountability** to guide the creation and deployment of ML systems in an organization.

Why is it important?
By definition, ML governance **should close the gap that exists between accountability and ethics in technological advancement**. It makes sure that boundaries within technology are set, so it does no harm and further aggravate inequalities incidentally while it operates.

In a business context we use it for safeguard investments and provide a good ROI (Return on Investment). Business better be maintaining a sustainable profit.

Shareholders / users need clear visibility that customters/users/employers/employees and regulatory bodies are content/comfortable.

Why should we use it?
For our community this is about good housekeeping with an added focus on mitigating the inherent risks of ML, addressing topics such as **data provenance**, **transparency**, **bias**, **performance management**, and **reproducibility**.

Propose to use 'Staged ML Governance'

We don't want to throw a pre-defined governance model at everyone. Especially a model that covers items we aren't even working on. Therefore we propose to use a 'Staged ML Governance model'. We add governance as we move forward with building out our community and associated projects.

Stage 1 - every project has a git repo and a list of github users who have maintainer privileges. We are currently at Stage 1.

Stage 2 - every project has a github-org Project, with an associated github kanban board. This practice is in use for community projects such as os-climate and OSG.

Stage 3 - every project has a kube-sytle community repo and a SIG (Special Interest Group). See sample SIGS: sample1, sample2