Project Governance

OWASP Gen AI Security Project
(Top 10 List for LLM and Gen AI)

Version 2.0
February 2025

Table of Content

Introduction

The Gen AI Security Project (Top 10 for LLM and Gen AI) governance model is based on the Meritocratic governance model by Ross Gardler and Gabriel Hanganu. And is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.

This governance model outlines the structure and roles within the Project, ensuring transparency, fairness, and efficiency in decision-making while fostering a thriving and collaborative open-source ecosystem.

Roles and Responsibilities

The governance model is based on a meritocratic system, where contributions, expertise, and sustained participation determine decision-making authority and leadership roles.

Anyone with an interest in the project can join the community, contribute to the project design and participate in the decision making process. This document describes how that participation takes place and how to set about earning merit within the project community.

Board of Directors

The Board of Directors (BoD) serves as the highest decision-making body, ensuring the long-term sustainability and strategic alignment of the project.

Membership:

Anyone can become a member; there are no special requirements, other than to have shown a willingness and ability to participate in the project as a team player, demonstrate subject matter expertise, and be recognized as providing significant strategic and material contributions to the project.

1. Responsibilities:
    a. Establish and uphold the vision, mission, and values of the project.
    b. Approve budgets, financial plans, and funding allocations.
    c. Resolve disputes and make final decisions on governance and project matters.
    d. Appoint or confirm leadership roles within the project.
    e. Represent the project to external stakeholders, including sponsors and partners.

f.

2. Term and Appointment

    a. 2 year staggered terms to ensure board continuity
    b. Elected by a Simple Majority of the current BoD and CPMT members
    c. Members can be removed by a ⅔ majority vote of the board.

Core Project Management Team

The Core Project Management Team (CPMT) is responsible for the project's ongoing management, coordination, and development. The core team members are expected to review code contributions, participate in strategic planning, approve changes to the governance model and manage the copyrights within the project outputs.

Members of the Core Team do not have significant authority over other members of the community, although it is the CPMT that votes on new team members and project Initiatives. See Initiatives, for further details.

Anyone can become a member; there are no special requirements, other than to have shown a willingness and ability to participate in the project as a team player. Typically, a potential member will need to show that they have an understanding of the project, its objectives and its strategy. They will also have provided valuable contributions to the project over a period of time.

Core project team members are made up of actively contributing project members who are either/or:

- Operational or Technical Lead fulfilling a specific role - appointed by the board
- Initiative lead (manages a specific approved project initiative)

    Responsibilities:

    - Maintain project infrastructure and ensure operational continuity.
    - Oversee contributions, code quality, and project roadmaps.
    - Communicate important project updates to the community.
    - Approve new Initiatives

    Term and Appointment

    - No specific term is currently determined, though the desired term is 1 year.
    - Appointed by the board of directors
    - Successfully propose new initiative for the project
    - Removal by ⅔ majority of the board.

Community Members and Contributors

Members and Contributors play vital roles in the project's ecosystem, Anyone can become a member; there are no special requirements, other than to have shown a willingness and ability to participate in the project as a team player. Typically, a potential member will need to show that they have an understanding of the project, its objectives and its strategy. Below we outline the potential roles and responsibilities members can take within the community.

Users

Users are community members who have a need for the project. They are the most important members of the community and without them the project would have no purpose. Anyone can be a user; there are no special requirements.

The project asks its users to participate in the project and community as much as possible. User contributions enable the project team to ensure that they are satisfying the needs of those users.

Contributors

Contributors are community members who contribute in concrete and substantial ways to the project. Anyone can become a contributor, and contributions can take many forms. There is no expectation of commitment to the project, no specific skill requirements and no selection process..

Reviewers

Reviewers primarily focus on reviewing contributions and providing feedback as part of an initiative, committee or working group.

Experts

Expert contributors are individuals with specialized knowledge in critical domains such as cybersecurity, generative AI, or other fields necessary to support the goals of specific working groups or committees and have shown continued significant contribution to the project.

Expert Review Board

An expert review board is a designated set of distinguished experts who may not be traditional contributors but may bring specific expertise to be used as a sounding board or help to validate output from an Initiative. An initiative lead may form a review board based on the needs of their Initiative.

Committees / Working Groups

Working Groups are formed at the direction of the BoD and support specific initiatives or committees. Anyone can join a working group and offer to contribute their time and expertise in alignment with the charter and focus for the Initiative or committee.

Decision-Making Process

Decisions are made based on merit, expertise, and consensus. Decisions about the future of the project are made through discussion with all members of the community, from the newest user to the most experienced Core Team member. All non-sensitive project management discussion takes place on the project contributors' Slack. Occasionally, sensitive discussion occurs on a private list.

The following principles guide the decision-making process:

1. Consensus-based decision-making: Discussions aim to achieve general agreement among stakeholders.

2. Escalation protocol: If consensus cannot be reached, the decision is escalated to the Initiative Lead, then the Core Project Management Team, and, if necessary, the Board of Directors.

3. Transparency: All major decisions are documented and shared publicly.

In order to ensure that the project is not bogged down by endless discussion and continual voting, the project operates a policy of lazy consensus. This allows the majority of decisions to be made without resorting to a formal vote.

Lazy Consensus

Lazy consensus decision making typically involves the following steps. Proposal, Discussion, Vote (if consensus is not reached through discussion), Decision.

Any community member can make a proposal for consideration by the community. In order to initiate a discussion about a new idea, they should send a slack to the project contributors' list or submit a patch implementing the idea to the issue tracker. This will prompt a review and, if necessary, a discussion of the idea. The goal of this review and discussion is to gain approval for the contribution. Since most people in the project community have a shared vision, there is often little need for discussion in order to reach consensus

For lazy consensus to be effective, it is necessary to allow at least 72 hours before assuming that there are no objections to the proposal. This requirement ensures that everyone is given enough time to read, digest and

respond to the proposal. This time period is chosen so as to be as inclusive as possible of all participants, regardless of their location and time commitments.

Voting

Not all decisions can be made using lazy consensus. Issues such as those affecting the strategic direction or legal standing of the project must gain explicit approval in the form of a vote. Every member of the community is encouraged to express their opinions in all discussions and all votes. However, only project Initiative Leads, CPMT, and/or BoD members (as defined above) have binding votes for the purposes of decision making.

Unless otherwise specified, decisions by vote at a meeting will require a simple majority vote, provided quorum is met. Decisions by electronic vote without a meeting will require a majority of all voting representatives.

Quorum for the BoD and CPMT is 51% or more of the total group present, for decision making Votes.

Contribution Guidelines

Anyone can contribute to the project, regardless of their skills, as there are many ways to contribute. For instance, a contributor might be active on the project slack and issue tracker, or might supply patches.

Contributors and reviewers will be acknowledged by being listed in the published work they contributed to or reviewed.

Project Initiatives

"Initiatives" within the project refer to structured activities that align with the project's goals and objectives while extending its scope through various deliverables or contributions. These initiatives, such as research collaborations or methodology development, operate under the project banner but have flexibility in defining their own outputs, which may include whitepapers, code, workshops, or other resources.

The governance process requires submitting a proposal detailing goals, deliverables, team members, and resource needs, followed by core team review and a voting process for approval. Once approved, initiatives must adhere to reporting responsibilities, including bi-weekly updates and active collaboration within designated channels.

Initiative Lead

Initiative Leads manage specific major initiatives (focused working groups) within the project. See the initiative governance guidelines for details on Initiative governance.

Responsibilities:

- Define goals, roadmaps, and deliverables for their respective initiatives.
- Coordinate with contributors, reviewers, and working groups.
- Ensure timely execution of tasks within their initiative.
- Regularly report progress to the Core Project Management Team and on the bi-weekly Open project review meetings.

Appointment:

- Initiative leads are appointed based on a successful proposal, vote and approval of a new project initiative.
- Initiative leaders can be removed by a 2/3rds majority vote of the Core Project Management Team, or the board of directors.

Initiative Governance

The general process for submission, review and approval requires creation of an initiative proposal, identification of the core contributing team members, and a roadmap of deliverables which is reviewed by the project core team and put to a open vote of the core team after review and any refinement of the proposal doc to confirm approval of the project.

Initial Submission

1. Complete Initiative Proposal One/Two Pager
    - The first step for each initiative is to create a version of the initiative proposal document that outlines the goals, objectives, specific outcomes and/or artifacts and a roadmap.
    - Include the name of the individual or individuals if proposing jointly.
    - Initiative costs, if required. All initiatives should have a $0 version of the proposal.
    - Resourcing: identify existing execution team, if there is one or if there is need for recruitment.
    - Proposal Starter Template: https://docs.google.com/document/d/1eaBbc_oVZISrNkp-VDgU4oRohV1cbbJGyNWPIhVT4kE/edit?usp=sharing

Proposal Review

Proposal to be reviewed by the core team for initiative alignment, evaluate and review resourcing, recruitment needs and any funding requirements, if requested.

- There may be requests to modify the proposal made by core team members.
- There will be a goal for a fixed period for review to not exceed 4 weeks, unless changes and change requests require additional research and development.
- Final Reviewed Submission
- Revised initiative proposal is submitted for approval.
- Share to the CPMT #team-llm-core. channel

Approval Requirements

- Reviewed Initiative Final Proposal, Committed Roadmap & Dates
- Identified core contribution and development team resources
    - Must meet minimally viable # of contributors to meet committed roadmap deliverables and deadlines.
- Budget requirement/requests (testing infrastructure, sw licensing, etc)

Approval Process

- Simple majority vote of the CPMT members and BoD.
- The vote remains open for 72 hours to allow time for review and support globally distributed teams.

Retirement of an Initiative

An initiative may be retired if its lead steps down and no replacement is found or if it becomes inactive. The Board will decide in either case.

Licensing and Attribution

The project develops and distributes content under approved OSI licensing models for both “Content” and “Code” assets. The project favors support for highly Permissive licenses to ensure the broadest accessibility and usability without restriction to the work of the expert community.

All Content

The project produced "Content" materials are by default distributed under Creative Commons Attribution-ShareAlike 4.0 International License. These include documents, images, reports, spreadsheets , JSON, partial code examples, and framework artifacts and other materials which are not executable code.

Below are summarized the licensing details for Creative Commons 4.0 for the project as well as a link to the full CC license agreement.http://creativecommons.org/licenses/by-sa/4.0/

Acceptable OSI Licenses for "Executable Code", "Binaries", ect.

For executable code and binaries the project, as mentioned earlier, prefers the use of the most Permissible OSI approved licenses.

Prefered OSI licences for the project include the following:

BSD - Berkeley Software Distribution License
MIT - Massachusetts Institute of Technology - Open Source Licence
Apache 2.0 - Apache Foundation License

Content Usage and Project Representation

All members of the project are encouraged to use , share and promote content published by the project under the terms of the CC licensing agreement and extend it with their personal voice, however only project officers and or identified individuals can speak for the Project and represent or issue formal, official communications issued by OWASP. More information can be found in the "Project Communications Guide".

Amendments and Evolution

This governance document may be revised as needed to reflect the evolving needs of the project. The Board of Directors may unilaterally revise the governance at any time. Any additional proposed changes must be reviewed by the Core Project Management Team and ratified by the Board of Directors.

This governance model ensures an open, fair, and sustainable ecosystem where contributors are recognized for their efforts, and leadership is determined based on merit and community trust.