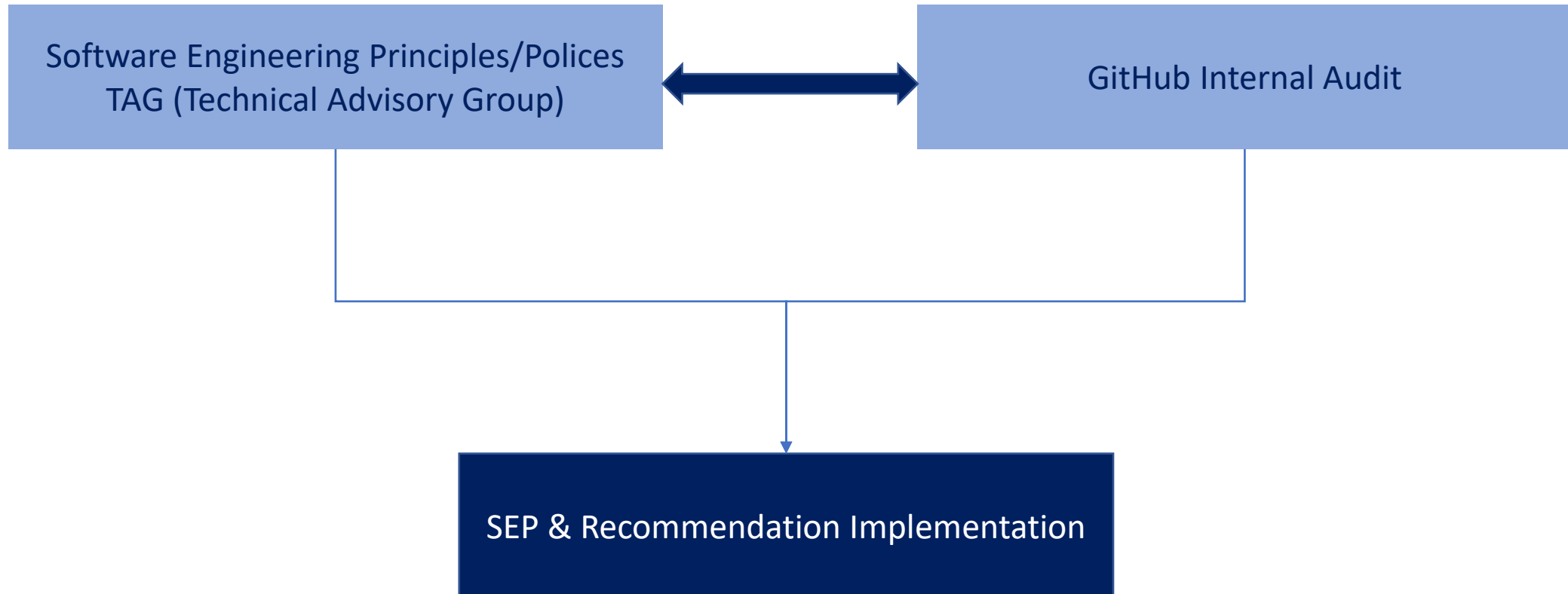


GitHub Policy

Action Plans

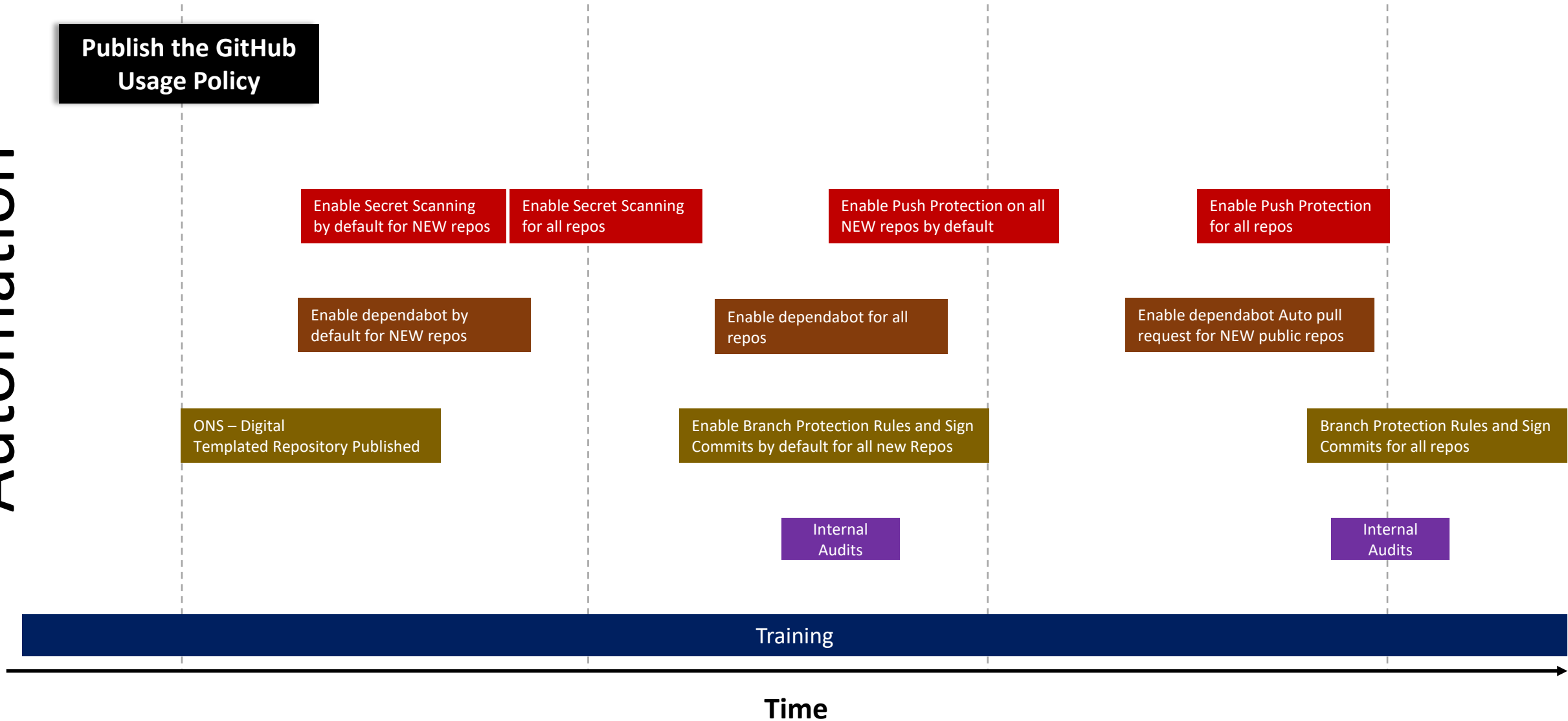
Implementation Planning



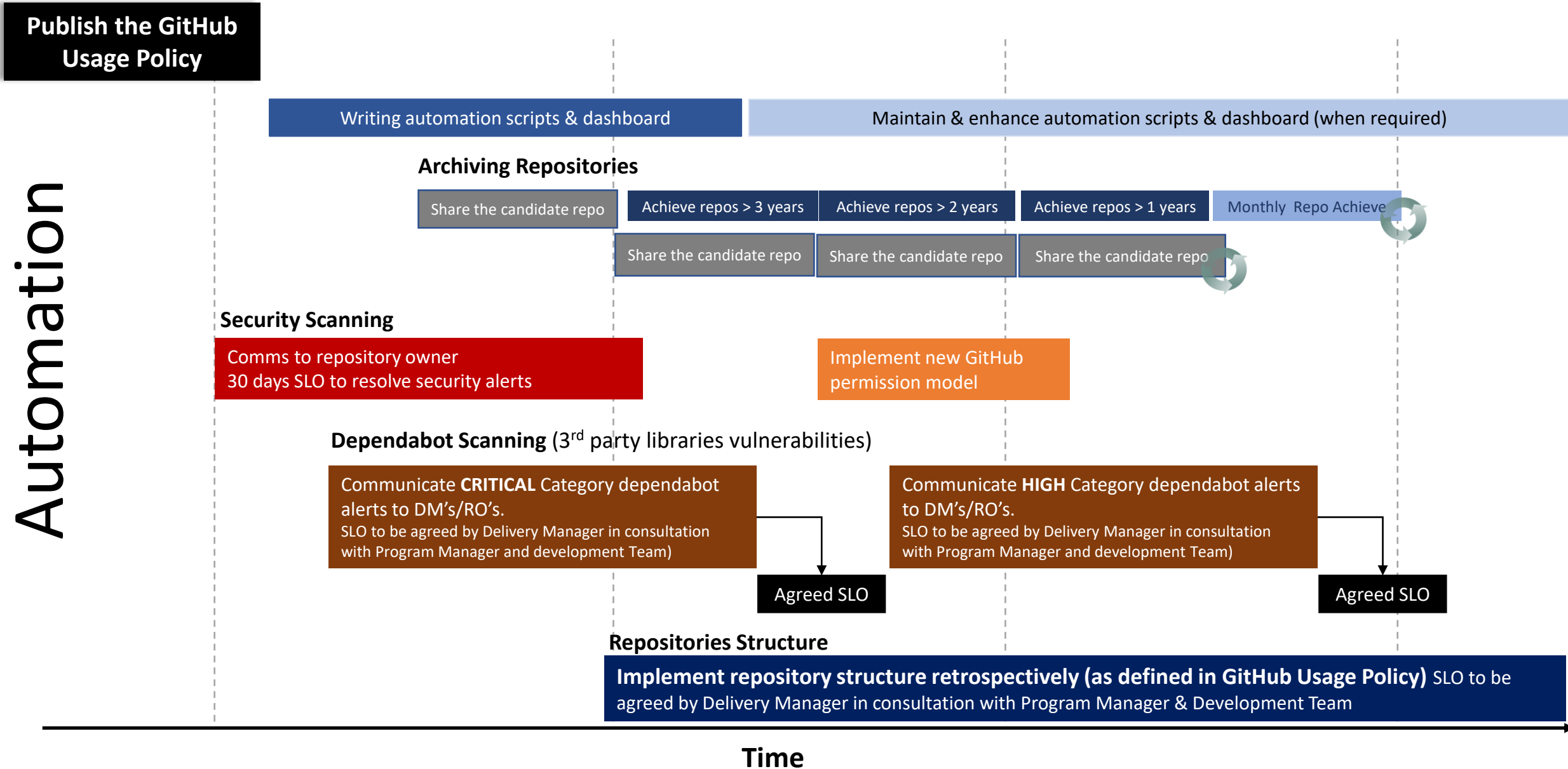
GitHub Usage Policy Implementation

Action Points for Now & Future

Automation



GitHub Usage Policy Retrospective Implementation - Action Points



GitHub Roles....

Organisational Owners

Complete administrative access to the organisation; limited to, but not less than, two people in the organisation

Team

Custom role for “Members with Admin Permission”, following permission attached to the role

- Admin: Create Repositories, Manage repository settings, including adding collaborators and setting their permissions, Create and Manage GitHub Teams
- Read: Access to view code, pull requests, and manage issues.
- Write: Ability to push to the repository and merge pull requests.
- Maintain: Manage project without full access to sensitive or destructive actions.
- Triage: Manage issues and pull requests without write access.

Technical
Leads Team

GitHub App Manager

Manage the settings of some or all GitHub App registrations owned by the organisation; Does not grant access to install and uninstall GitHub Apps on an organisation

Members

Default, non-administrative role for individuals in the organisation; has permissions such as creating repositories and project boards

Security Manager

Permissions to manage security alerts and settings across the organization, as well as read permissions for all repositories in the organisation.

Team