OSPO CON @ THE LINUX FOUNDATION OPEN SOURCE SUMMIT NORTH AMERICA

DIGITAL SERVICE AT CMS

Establishing a Baseline: Repository Maturity Models, Templates, Checklists & Metrics

Digital Service at The Centers for Medicare & Medicaid Services (CMS.GOV)
Natalia Luzuriaga, Isaac Milarsky, Remy DeCausemaker, Aayat Ali

https://github.com/DSACMS/decks/ossna24-baseline.pdf
opensource@cms.hhs.gov

CMS Open Source Program Office (OSPO)

Remy DeCausemaker
Open Source Team Lead

Aayat Ali
UX Designer

Natalia Luzuriaga
US Digital Corps Fellow

Isaac Milarsky
US Digital Corps Fellow

CodingItForward Fellow ‘24
Full-Stack Developer

CodingItForward Fellow ‘24
Full-Stack Developer

CodingItForward Fellow ‘24
Full-Stack Developer

DIGITAL SERVICE AT CMS

CMS Open Source Repository Baselines Overview: repo-scaffolder

Open Source Repository Maturity Models

- Where is our project on our Open Source Journey?
- **https://github.com/dsacms/repo-scaffolder/blob/main/maturity-model-tiers.md**

Repository Templates

- What files are required/recommended for healthy repository hygiene?
- **https://github.com/DSACMS/repo-scaffolder/tree/main/tier3/{{cookiecutter.project_slug}}**

Outbound Checklists

- What steps should our project take to release the repository publicly?
- **https://github.com/dsacms/repo-scaffolder/blob/main/tierX/checklist.pdf**

Cookiecutter

- How do we know what Maturity Model Tier our project should be in? What files are required in that Tier?
- `cookiecutter https://github.com/DSACMS/repo-scaffolder --directory=tierX`

Repolinter Configs

- What files or information is missing from our repo?
- **https://github.com/DSACMS/repo-scaffolder/blob/main/tier1/{{cookiecutter.project_slug}}/repolinter.json**

Open Source Program Office (OSPO) at CMS

1. About the OSPO
2. How we grow the program
3. How we reduce duplicate work
4. How we reduce risk

What does the Digital Service at CMS.gov do?

The Digital Service at the Centers for Medicare & Medicaid Services transforms the U.S. Healthcare system by deploying design, engineering, product, and policy experts on a 'tour of duty' alongside dedicated civil servants.

We bring industry best practices and fresh approaches government modernization, to help solve some of the most complex problems facing healthcare today.

Who we serve: The American People

65 M

Medicare Beneficiaries

(2022)

88 M

Medicaid Beneficiaries

(2022)

31 M

Healthcare.gov

(2021)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: Taxpayers

$ 1.7 T

CMS Budget - 12% of the federal budget

(FY 2022)

$ 829 B

Total Medicare Payments

(FY 2021)

$ 646 B

Total Medicaid Payments

(FY 2019)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: The Health Care System

6,244

CMS Employees

(FY 2022)

1.4M

Health Care Providers

(2022)

20%

National Health Care Spending is Medicare

(2022)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

How do we ‘do’ Open Source at CMS?

Policies

How we **inbound** and **outbound** open source contributions and content

Projects

How we **solve real-world problems** by working in the open

Programs

How we **measure**, and **manage** contributors, projects, **risks**, and **opportunities**

How does our OSPO provide value?

Save us Money

Save us Time

Accountability for Contract Performance

Engine for Talent

Reduce Duplicate Work

Reduce Duplicate Costs

Reduce Security Risk

Reduce Continuity Risk

How we grow the program

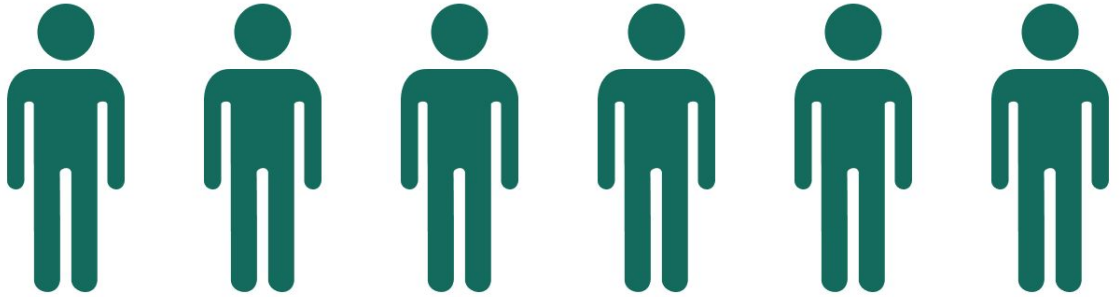
Engine for Talent

DIGITAL SERVICE AT CMS

Early Career Talent Pipeline at the Digital Service

Digital Service at CMS.gov DIGITAL SERVICE AT CMS	**Up to 4 year tour of duty** for established professionals in **Engineering, Product management, Design, and Data science**. GS-13+	https://cms.gov/digital-service-cms
DigitalCorps at GSA.gov UNITED STATES DIGITAL CORPS	**2 year tour of duty** for **early-career** technologists, eligible to convert to full-time, career positions in the competitive service at their agency. GS-9 to 12, + **50% recruitment Incentive**.	https://digitalcorps.gsa.gov
Civic Digital Fellowship at CodingItForward.com CIVIC DIGITAL FELLOWSHIP	**Paid 10 week summer internship** program for **currently enrolled** undergrad, grad, bootcamp students **or recent graduates**.	https://www.codingitforward.com
Urban Alliance URBAN ALLIANCE	**6 month part-time to full-time Program** that provides skills training, mentoring, and **paid internships** to high school seniors that keep them connected to school or the workforce.	https://urbanalliance.org

Early career talent pipeline Demographics



6 Interns & Fellows

3 Coding it Forward Fellows

2 Digital Corps Fellows

1 Urban Alliance Intern

5 out of 6

identify as women

Projects

Released 12

open source repositories in the past year

How we reduce duplicate work

Repository Maturity Models & Cookiecutter Configs

DIGITAL SERVICE AT CMS

CMS Open Source Repository Maturity Model (v1)

Spreadsheet/PDF presented at GitHub Universe 2023 OSPO WG

	Ordinality of Documentation By Tier (M - Mandatory, R - Recommended, N - Not Recommended)				
File	Tier 0: Private Repo	Tier 1: One-time Release	Tier 2: Close Collaboration	Tier 3: Working in Public	Tier 4: Community Governance
LICENSE	M	M	M	M	M
SECURITY.md	N	M	M	M	M
README.md	M	M	M	M	M
CONTRIBUTING.md	R	R	M	M	M
MAINTAINERS.md	N	N	R	M	M
GOVERNANCE.md	N	N	N	R	M
CODEOWNERS.md	N	N	R	M	M
COMMUNITY_GUIDELINES.md	N	N	M	M	M
CODE_OF_CONDUCT.md	N	N	M	M	M

CMS Repository Cohort Definitions: Maturity Model Tiers

Level	Name	Purpose	Description
Tier 0	**Private Repository**	Experimental, Historical	Project is **private**, usually with a single developer. Typically **working projects**, example code, and **early prototypes**.
Tier 1	**One-Time Release**	Publication for Informational, Accountability, Transparency Purposes	Project released publicly, but ***without planned future activity*** or maintenance from original author(s).
Tier 2	**Close Collaboration**	Collaboration with smaller, mostly internal teams	Project within a team or Operational Division (OpDiv), Internal Repo for ***Innersource-style work.***
Tier 3	**Working in Public**	Collaboration in the open with smaller, semi-open teams	Project developed Open Source by CMS or a CMS contractor, public website hosted on GitHub, tool or utility used in CMS official business by the public. ***Limited external contribution, CMS-led (by choice or by statute).***
Tier 4	**Community Governance**	Collaboration broadly in public	Project donated to or stewarded by an external community, open standard that welcomes public input, mature open source project that purposefully develops an ***open governance structure***.

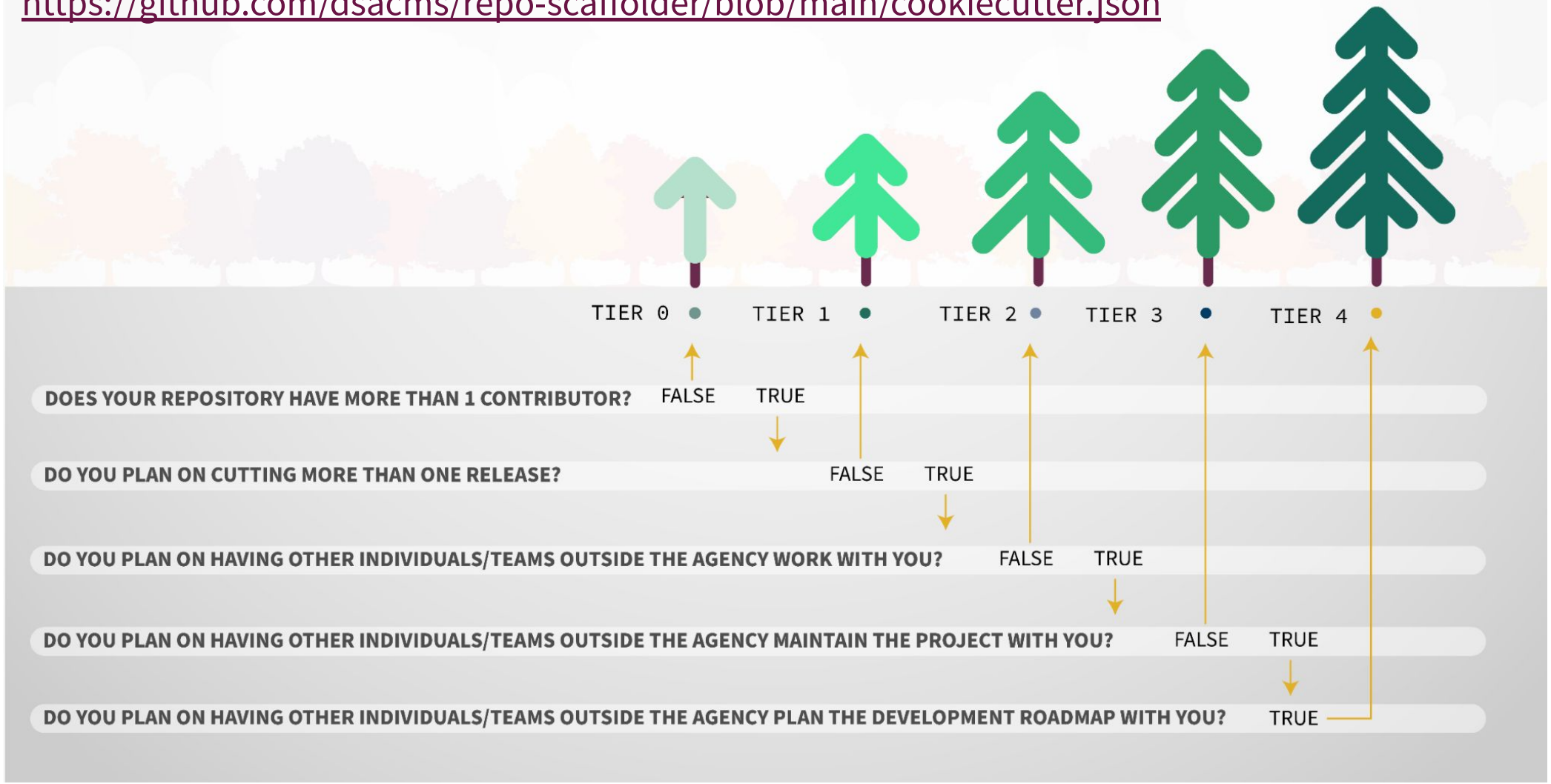
CMS Open Source Repository Maturity Model (v2)

Public Repo on GitHub!
https://github.com/dsacms/repo-scaffolder/blob/main/maturity-model-tiers.md

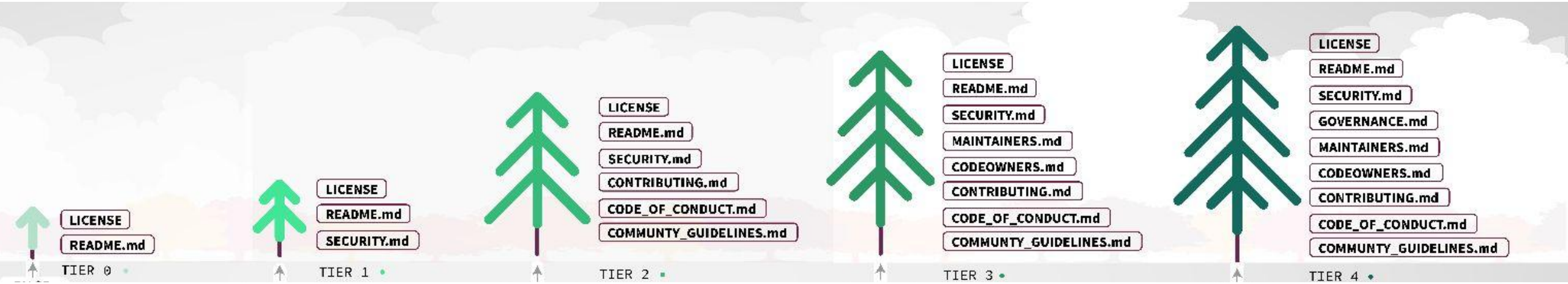
File	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4
LICENSE	M	M	M	M	M
SECURITY.md	N	M	M	M	M
README.md	M	M	M	M	M
CONTRIBUTING.md	R	R	M	M	M
MAINTAINERS.md	N	N	R	M	M
GOVERNANCE.md	N	N	N	R	M
CODEOWNERS.md	N	N	R	M	M
COMMUNITY_GUIDELINES.md	N	N	M	M	M
CODE_OF_CONDUCT.md	N	N	M	M	M

cookiecutter command-line tool v2: Tier-selection config

https://github.com/dsacms/repo-scaffolder/blob/main/cookiecutter.json



cookiecutter command-line tool v2: Tier-specific configs



cookiecutter templates:
https://github.com/dsacms/repo-scaffolder/blob/main/tier0/cookiecutter.json
https://github.com/dsacms/repo-scaffolder/blob/main/tier1/cookiecutter.json
…

How we reduce risk

Outbound Repository Checklists, Metrics, and Linters

DIGITAL SERVICE AT CMS

Outbound Review Checklists

Tier1 - “One-Time Release”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier1/checklist.pdf

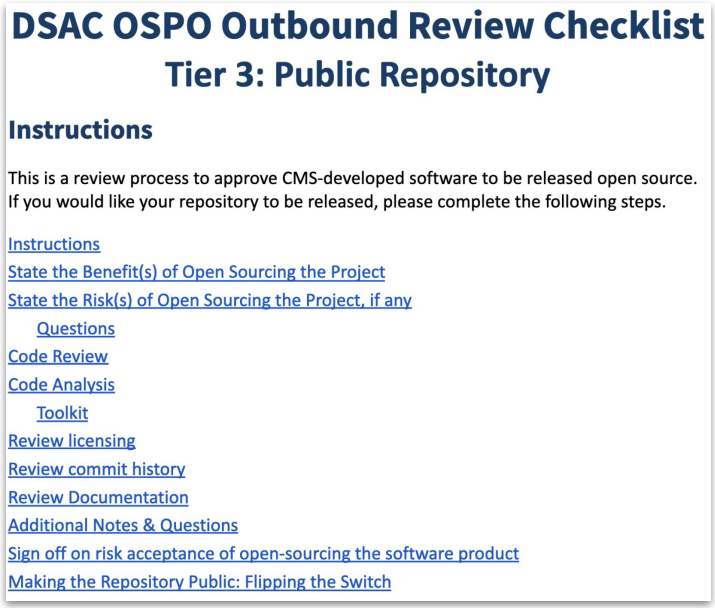
Tier3 - “Working In Public”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

Tier4 - “Open Governance”
https://github.com/DSACMS/repo-scaffolder/blob/main/tier4/checklist.pdf

Coming Soon!

- Tier2 - “Close Collaboration”
  - innersource patterns!

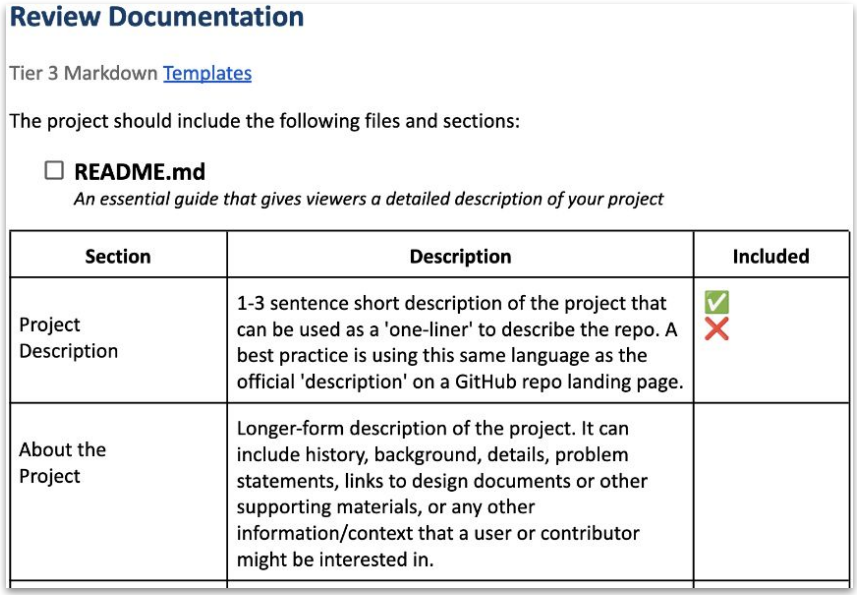
Outbound Review Checklists



DSAC OSPO Outbound Review Checklist
Tier 3: Public Repository

Instructions

This is a review process to approve CMS-developed software to be released open source. If you would like your repository to be released, please complete the following steps.



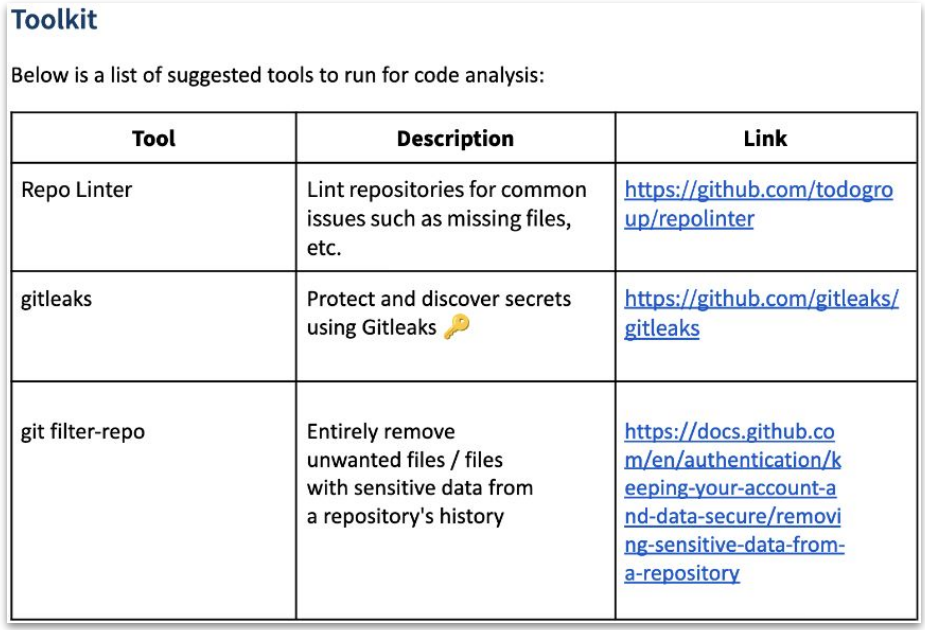
Review Documentation

Tier 3 Markdown Templates

The project should include the following files and sections:

☐ **README.md**
An essential guide that gives viewers a detailed description of your project

Section	Description	Included
Project Description	1-3 sentence short description of the project that can be used as a 'one-liner' to describe the repo. A best practice is using this same language as the official 'description' on a GitHub repo landing page.	✅ ❌
About the Project	Longer-form description of the project. It can include history, background, details, problem statements, links to design documents or other supporting materials, or any other information/context that a user or contributor might be interested in.	



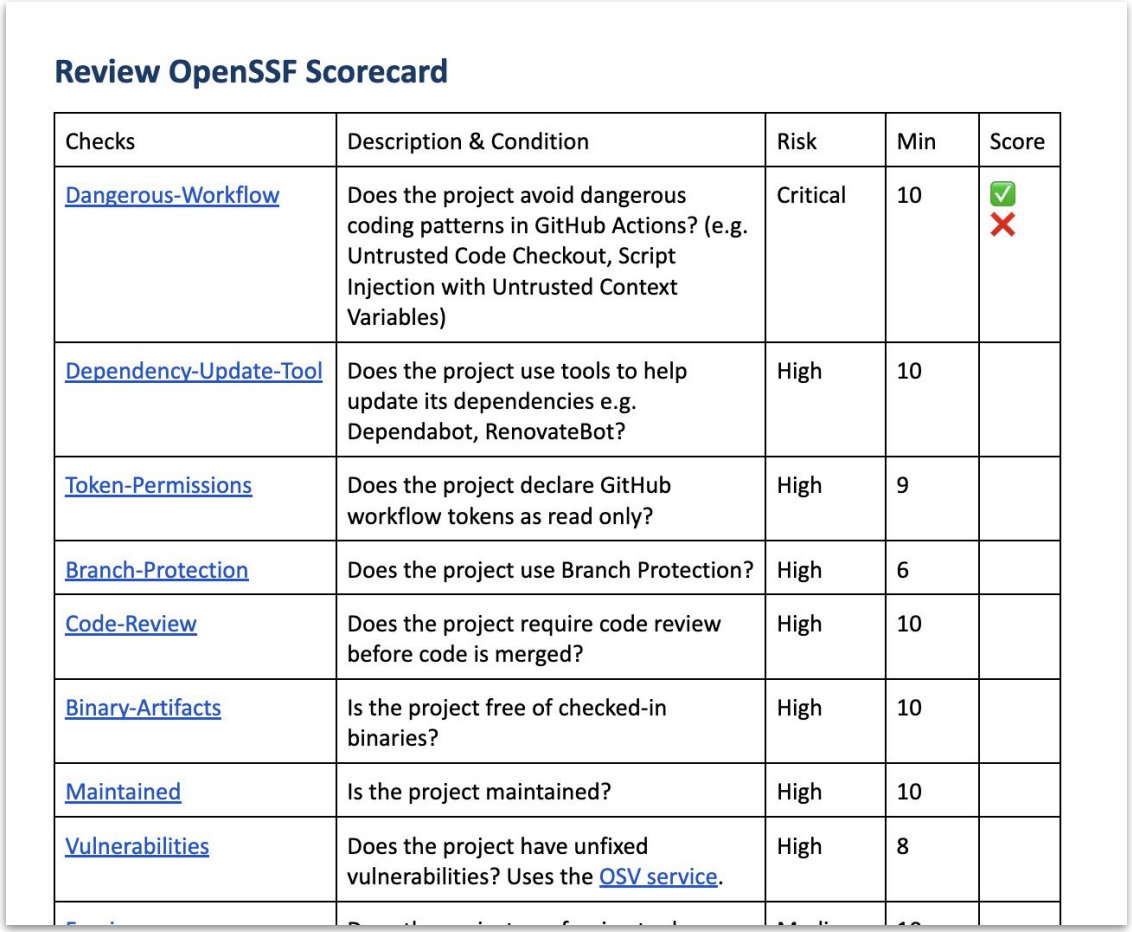
Toolkit

Below is a list of suggested tools to run for code analysis:

Tool	Description	Link
Repo Linter	Lint repositories for common issues such as missing files, etc.	https://github.com/todogroup/repolinter
gitleaks	Protect and discover secrets using Gitleaks 🔑	https://github.com/gitleaks/gitleaks
git filter-repo	Entirely remove unwanted files / files with sensitive data from a repository's history	https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository

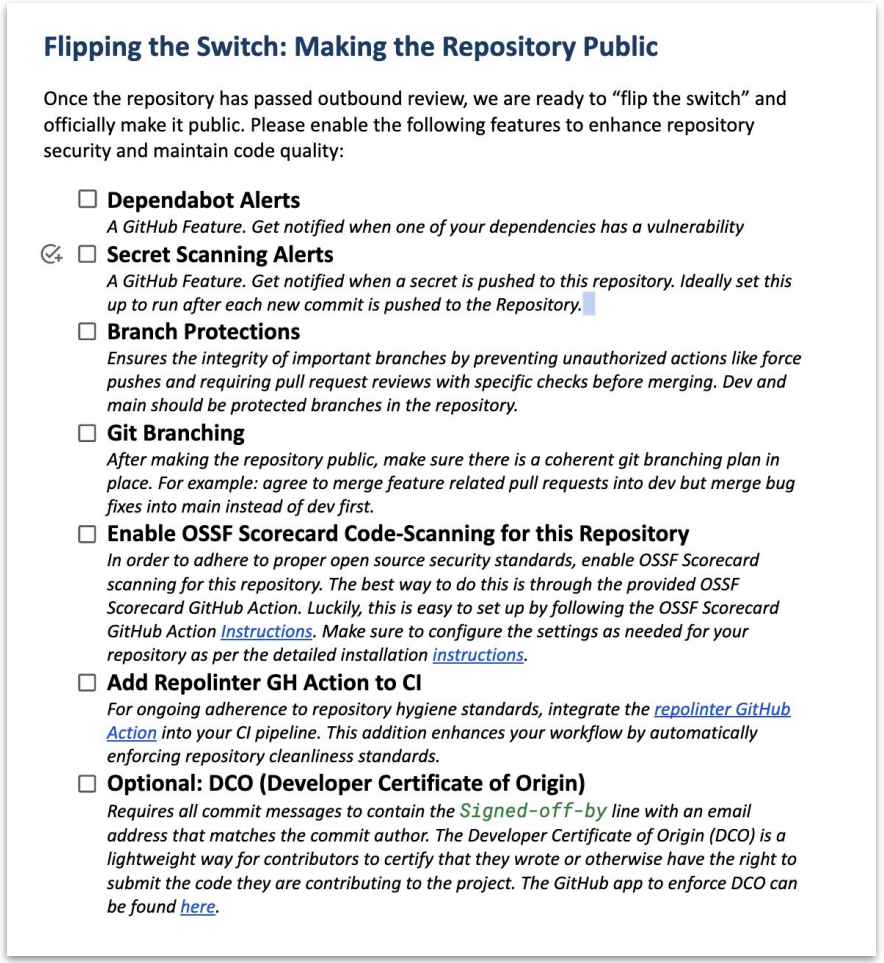
https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/checklist.pdf

Tier 4: Reviewing OpenSSF Scorecard



Review OpenSSF Scorecard

Checks	Description & Condition	Risk	Min	Score
Dangerous-Workflow	Does the project avoid dangerous coding patterns in GitHub Actions? (e.g. Untrusted Code Checkout, Script Injection with Untrusted Context Variables)	Critical	10	✅ ❌
Dependency-Update-Tool	Does the project use tools to help update its dependencies e.g. Dependabot, RenovateBot?	High	10	
Token-Permissions	Does the project declare GitHub workflow tokens as read only?	High	9	
Branch-Protection	Does the project use Branch Protection?	High	6	
Code-Review	Does the project require code review before code is merged?	High	10	
Binary-Artifacts	Is the project free of checked-in binaries?	High	10	
Maintained	Is the project maintained?	High	10	
Vulnerabilities	Does the project have unfixed vulnerabilities? Uses the OSV service.	High	8	



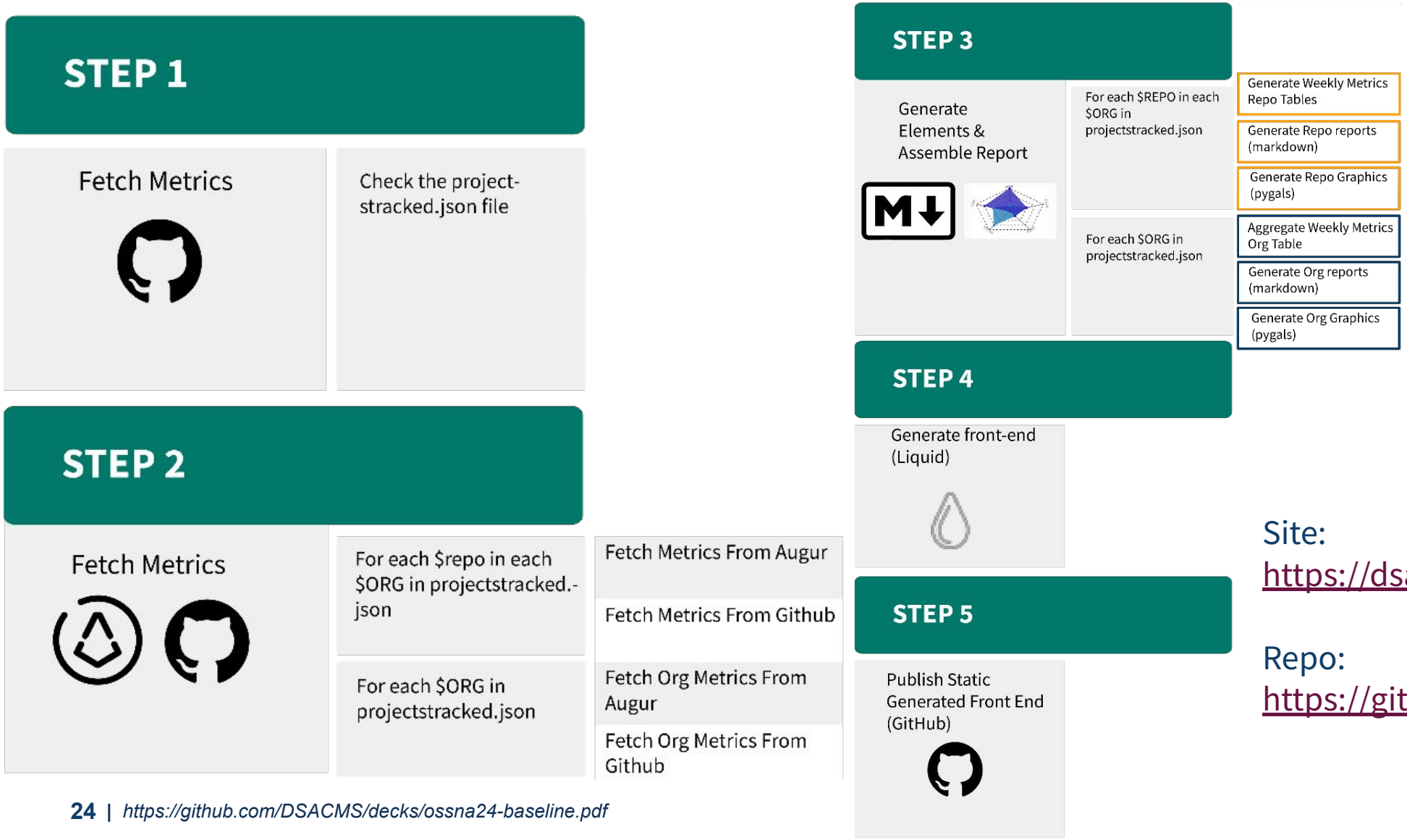
Flipping the Switch: Making the Repository Public

Once the repository has passed outbound review, we are ready to "flip the switch" and officially make it public. Please enable the following features to enhance repository security and maintain code quality:

- ☐ **Dependabot Alerts**
  A GitHub Feature. Get notified when one of your dependencies has a vulnerability
- ☐ **Secret Scanning Alerts**
  A GitHub Feature. Get notified when a secret is pushed to this repository. Ideally set this up to run after each new commit is pushed to the Repository.
- ☐ **Branch Protections**
  Ensures the integrity of important branches by preventing unauthorized actions like force pushes and requiring pull request reviews with specific checks before merging. Dev and main should be protected branches in the repository.
- ☐ **Git Branching**
  After making the repository public, make sure there is a coherent git branching plan in place. For example: agree to merge feature related pull requests into dev but merge bug fixes into main instead of dev first.
- ☐ **Enable OSSF Scorecard Code-Scanning for this Repository**
  In order to adhere to proper open source security standards, enable OSSF Scorecard scanning for this repository. The best way to do this is through the provided OSSF Scorecard GitHub Action. Luckily, this is easy to set up by following the OSSF Scorecard GitHub Action Instructions. Make sure to configure the settings as needed for your repository as per the detailed installation instructions.
- ☐ **Add Repolinter GH Action to CI**
  For ongoing adherence to repository hygiene standards, integrate the repolinter GitHub Action into your CI pipeline. This addition enhances your workflow by automatically enforcing repository cleanliness standards.
- ☐ **Optional: DCO (Developer Certificate of Origin)**
  Requires all commit messages to contain the `Signed-off-by` line with an email address that matches the commit author. The Developer Certificate of Origin (DCO) is a lightweight way for contributors to certify that they wrote or otherwise have the right to submit the code they are contributing to the project. The GitHub app to enforce DCO can be found here.

https://github.com/DSACMS/repo-scaffolder/blob/main/tier4/checklist.pdf

CMS Open Source Repo Metrics Back-end

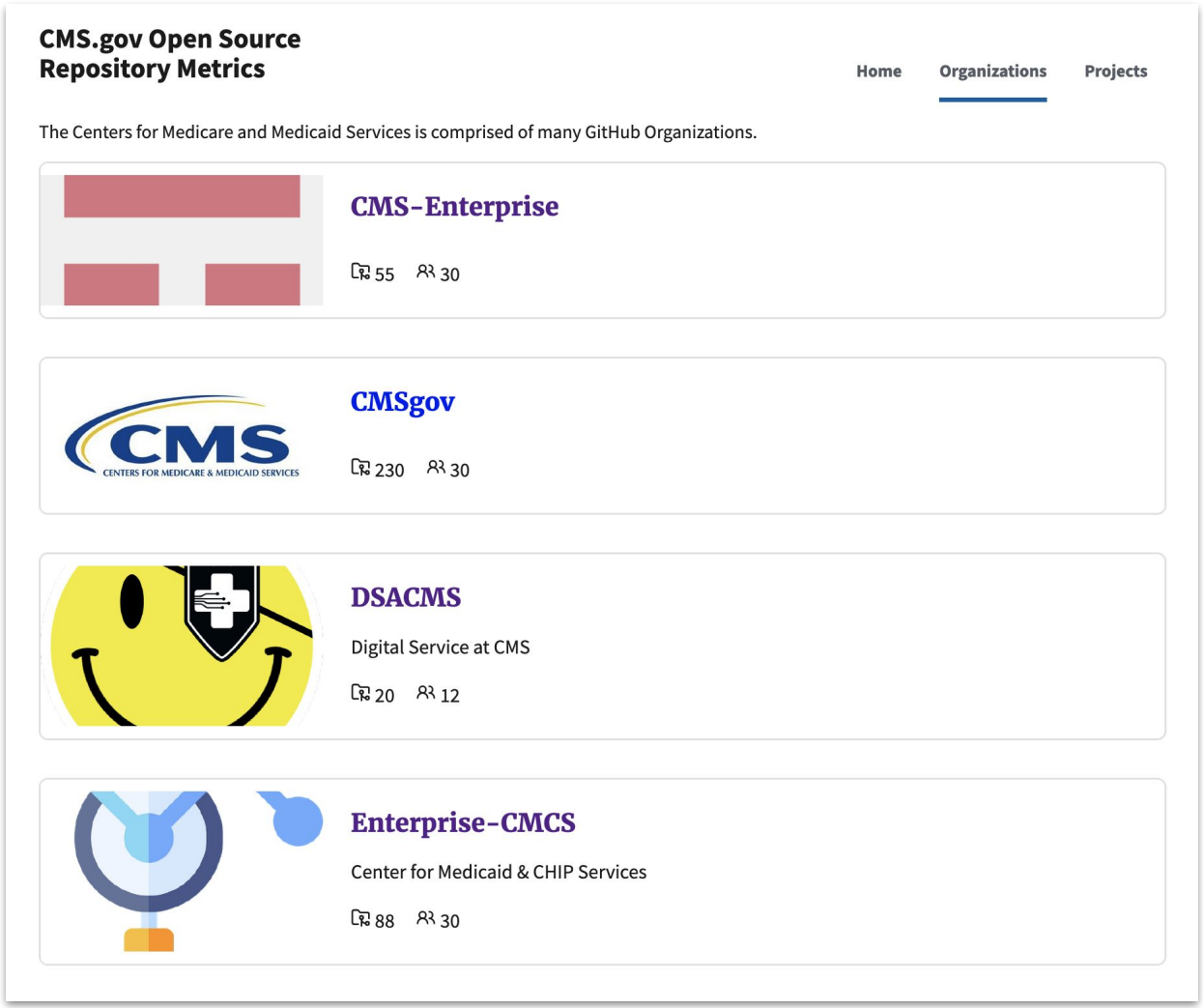


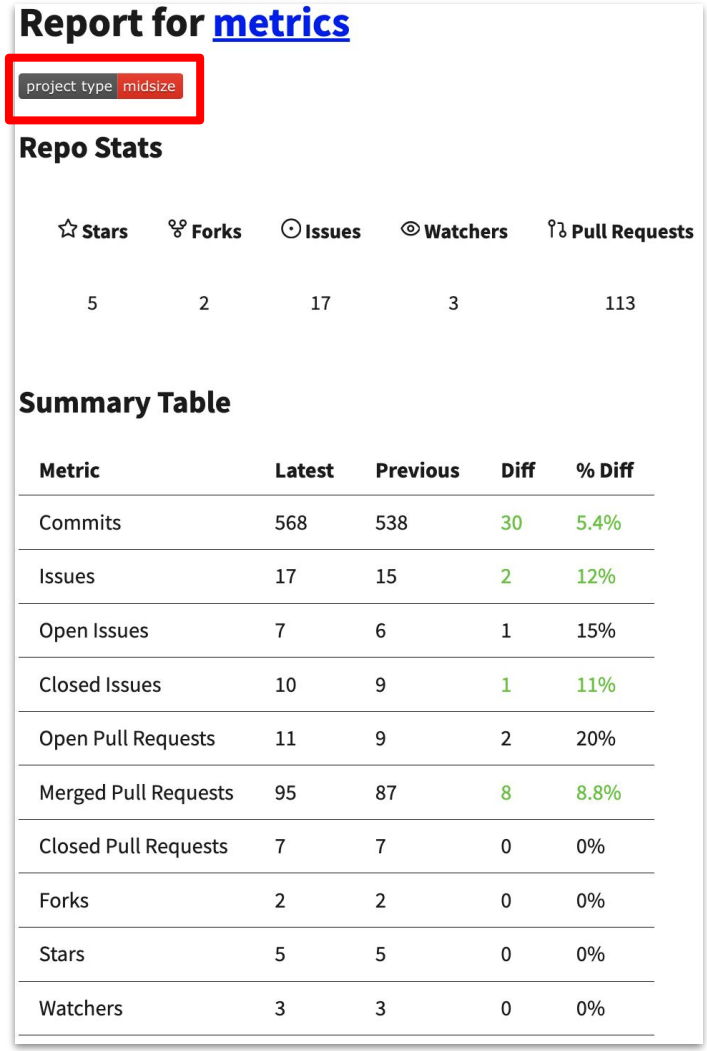
Site:
https://dsacms.github.io/metrics

Repo:
https://github.com/DSAMCS/metrics

DIGITAL SERVICE AT CMS

CMS.gov Open Source Repository Metrics Front-end (v1 released at OSSNA!)





THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

https://dsacms.github.io/metrics

CMS Repository Cohort Definitions: Nadia Labels

In her book "Working in Public" by Nadia Asparouhova classifies repositories into four cohorts:

- Toys
- Clubs
- Federations
- Stadiums

	HIGH USER GROWTH	LOW USER GROWTH
HIGH CONTRIBUTOR GROWTH	**Federations** (e.g., Rust)	**Clubs** (e.g., Astropy)
LOW CONTRIBUTOR GROWTH	**Stadiums** (e.g., Babel)	**Toys** (e.g., ssh-chat)

Various types of open source projects, classified by user and contributor growth.

https://project-types.github.io/

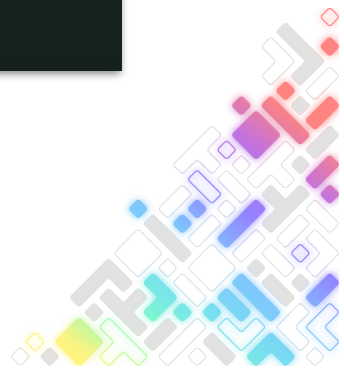
CMS Repository Cohort Definitions: Nadia Labels in Augur!

```
ratio_stargazers_to_contribs = stargazers_count / unique_contributor_count

if unique_contributor_count > 75 and ratio_stargazers_to_contribs < 2:
    return "club"
elif unique_contributor_count > 75 and ratio_stargazers_to_contribs > 2 and stargazers_count > 1000:
    return "federation"
elif unique_contributor_count < 6 and stargazers_count > 100:
    return "stadium"
elif unique_contributor_count < 6 and stargazers_count < 100:
    return "toy"

#"ContribMid" is the label for repos that don't make sense in the other
#categories. Contribs > 6 and < 75
return "contribMid"
```

See Augur API Documentation for nadia_project_labeling_badge:
https://github.com/chaoss/augur/blob/main/augur/api/metrics/repo_meta.py#L205



CMS Open Source Repository Maturity Model: Repolinter

https://github.com/todogroup/repolinter

Repolinter is a tool maintained by the TODOGroup for checking repositories for common open source issues, using pre-defined rulesets. This can be run stand-alone as a script, pre-commit in your IDE, or post-commit or within CI/CD systems!

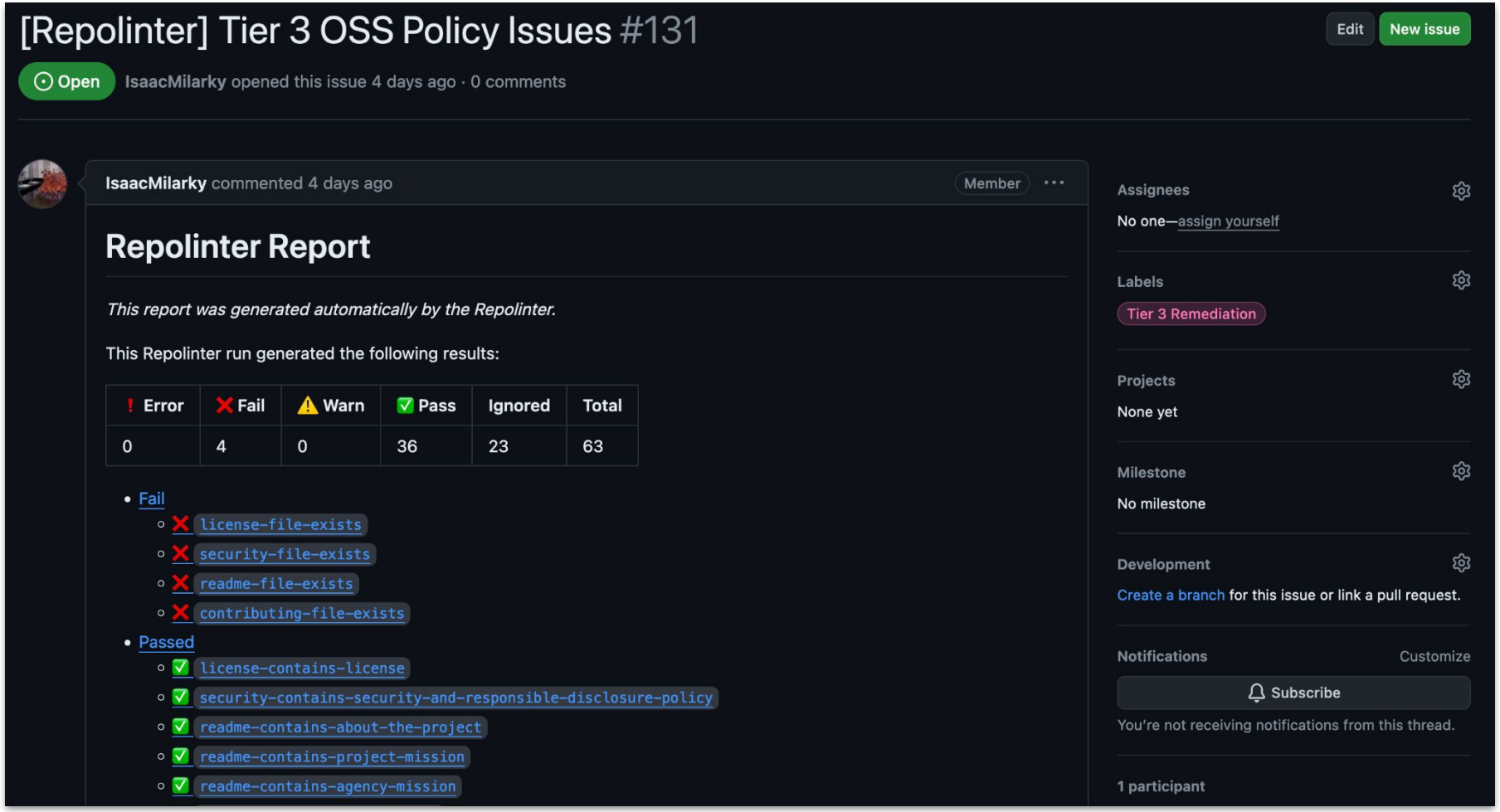
✔ = Pass
✖ = Fail
⚠️ = Warn

```
✔ license-file-exists: Found file (LICENSE.md)
✔ security-file-exists: Found file (SECURITY.md)
✔ readme-file-exists: Found file (README.md)
✔ contributing-file-exists: Found file (CONTRIBUTING.md)
✔ maintainers-file-exists: Found file (MAINTAINERS.md)
✖ codeowners-file-exists: Did not find a file matching th
⚠ governance-file-exists: Did not find a file matching th
✖ community-guidelines-file-exists: Did not find a file m
✖ code-of-conduct-file-exists: Did not find a file matchi
✔ license-contains-license: Contains license (LICENSE.md)
✔ security-contains-security-and-responsible-disclosure-p
✖ readme-contains-about-the-project: Doesn't contain Abou
```

Thanks to Chan and Satwic at the Comcast OSPO, we now have repolinter.json configs and rules that map to each Tier of our Open Source Repository Maturity Model!

https://github.com/DSACMS/repo-scaffolder/blob/main/tier3/%7B%7Bcookiecutter.project_slug%7D%7D/repolinter.json

CMS Open Source Repository Maturity Model: Repolinter



CMS Open Source Repository Baselines Overview: repo-scaffolder

Open Source Repository Maturity Models

- Where is our project on our Open Source Journey?
- **https://github.com/dsacms/repo-scaffolder/blob/main/maturity-model-tiers.md**

Repository Templates

- What files are required/recommended for healthy repository hygiene?
- **https://github.com/DSACMS/repo-scaffolder/tree/main/tier3/{{cookiecutter.project_slug}}**

Outbound Checklists

- What steps should our project take to release the repository publicly?
- **https://github.com/dsacms/repo-scaffolder/blob/main/tierX/checklist.pdf**

Cookiecutter

- How do we know what Maturity Model Tier our project should be in? What files are required in that Tier?
- `cookiecutter https://github.com/DSACMS/repo-scaffolder --directory=tierX`

Repolinter Configs

- What files or information is missing from our repo?
- **https://github.com/DSACMS/repo-scaffolder/blob/main/tier1/{{cookiecutter.project_slug}}/repolinter.json**

Acknowledgements & Attributions

The repo-scaffolder project originally began as a collaboration between the United States Digital Service (USDS.gov), The Department of Health and Human Services (HHS.gov), The Digital Service at the Centers for Medicare & Medicaid Services (CMS.gov), and The USDigitalResponse.org.

CMS would like to thank General Services Administration (GSA)'s 18F team, the Consumer Financial Protection Bureau (CFPB), and the Office of Management and Budget (OMB) for their inspirational work in the use of Free/Open Source Software in the Federal Government.

Our work continues to be guided by contributions from the CHAOSS OSPO Metrics Working Group and TODOGroup.org members.

Thank you!

Thank You

DIGITAL SERVICE AT CMS

creative commons

PUBLIC DOMAIN

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Questions or Comments?

https://github.com/DSACMS/decks/ossna24-baseline.pdf

Open Source Questions?

opensource@cms.hhs.gov

Digital Service Questions?

DigitalService@cms.hhs.gov

Help Answer the Call!

Digital Service at CMS.gov
https://cms.gov/digital-service

DigitalCorps Fellowships
https://digitalcorps.gsa.gov

CodingItForward Summer Internships
https://codingitforward.com