From Consumer to Steward

Standardizing Corporate Open Source Risk Practices

Daniel Izquierdo, Bitergia

Eclipse Community Day, Madrid
September, 2025

Daniel Izquierdo Cortázar

dizquierdo@bitergia.com

Ph.D in Empirical Software Engineering

CEO @ Bitergia

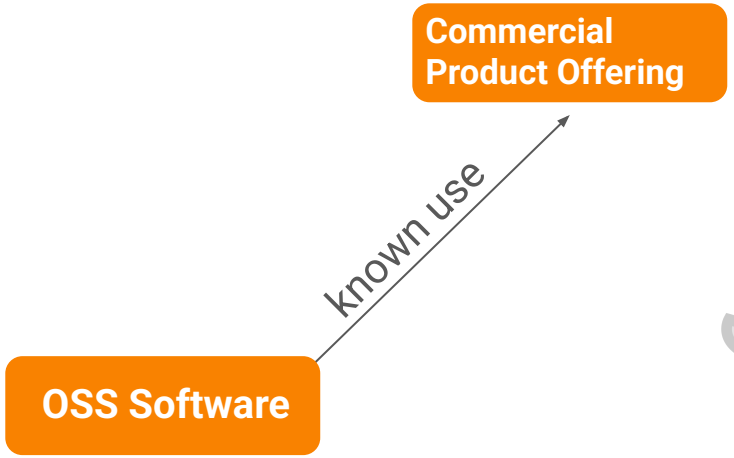
Chair @ InnerSource Commons Foundation

Board Member @ CHAOSS, Linux Foundation

Board Member @ Apereo Foundation

Open Source Software is everywhere

- Developers use open source software
- 70% - 95% of software includes open source



Most is under the surface - software supply chain

- Developers use open source software
- 70% - 95% of software includes open source
- Unmanaged OSS use → unknown dependencies

We need to make this unknown risk known

- Developers use open source software
- 70% - 95% of software includes open source
- Unmanaged OSS use → unknown dependencies → unknown risk

Definition: Software Bill of Material (SBOM)

An SBOM is a nested inventory, a list of ingredients that make up software components.

Motivation

- Corporations follow a **passive** approach, using or rejecting specific OSS components (e.g., CI/CD)
- But typically no ones cares about the sustainability of open source
- Can we grow a set of **industrial practices** (standards?) to make those projects more **sustainable** over time?

Challenges

- SBoM creation, immutability, and management
- Scale of the **SBoM** goes **over 100K OSS components**
- Be part of the conversation is time consuming
- There is **no** a **common vocabulary** for sustainability (automotive vs cloud ecosystems)
- No agreement on **how** to **detect risks** and define **mitigation strategies**
- **Unmaintained OSS projects or at risk is the norm, not the exception**

project: Kubernetes - Golang Deps × Add filter

Risk Model Overview Dashboard

Check the Risk Model Help Dashboard for more information about this analysis.

For more details, pin a filter by origin and visit the Risk Model Dashboard for Individual Projects.

Filters

Team

Select...

Project Category

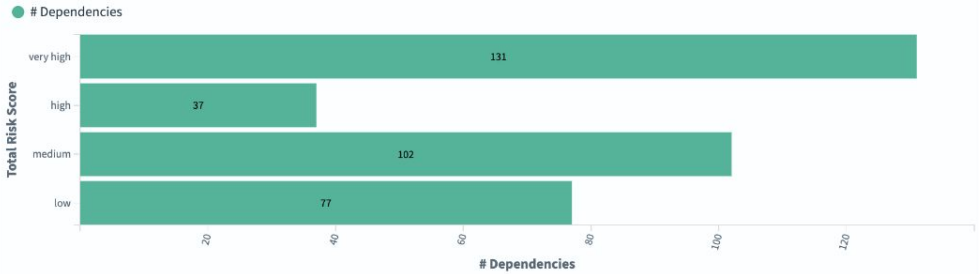
Kubernetes - Golang Deps ×

Overview

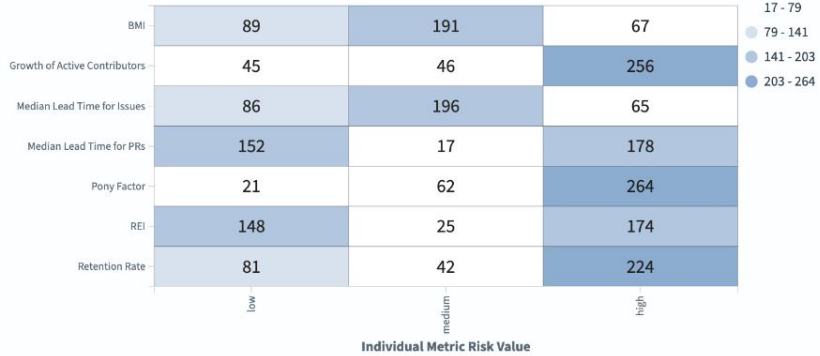
347
Dependencies analyzed

Bitergia
Team

Dependencies by Risk value



Risk Value per Metric, by number of Dependencies



Overall results by dependency repository

Filter...

Repository	Category	Risk Value	Risk Score (over 10)	# "Low risk" metrics	# "Medium risk" metrics	# "High risk" metrics	Last analyzed on
https://github.com/json-iterator/go	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/spf13/afero	Kubernetes - Golang Deps	very high	10	0	0	7	Jun 27, 2024 @ 12:35
https://github.com/Azure/go-ansiterm	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/ThalesIgnite/crypto11	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/coreos/go-semver	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/curioswitch/go-reassign	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/davecgh/go-spew	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35

Export: Raw Formatted

1 2 3 4 5 ... 50 »

Bitergia Analytics

Dashboards

project: Kubernetes - Gola

Risk Model Overvi

Check the Risk Model He

For more deta s, pin a f

Filters

Team

Select.

Project Category

Ku ernetes - Golang Deps ×

Risk Value per Metric, by numbe

Risk Value per Metric, by number of Dependencies

	Deps						12:35
https://github.com/coreos/go-semver	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/curioswitch/go-reassign	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35
https://github.com/davecgh/go-spew	Kubernetes - Golang Deps	very high	9.29	0	1	6	Jun 27, 2024 @ 12:35

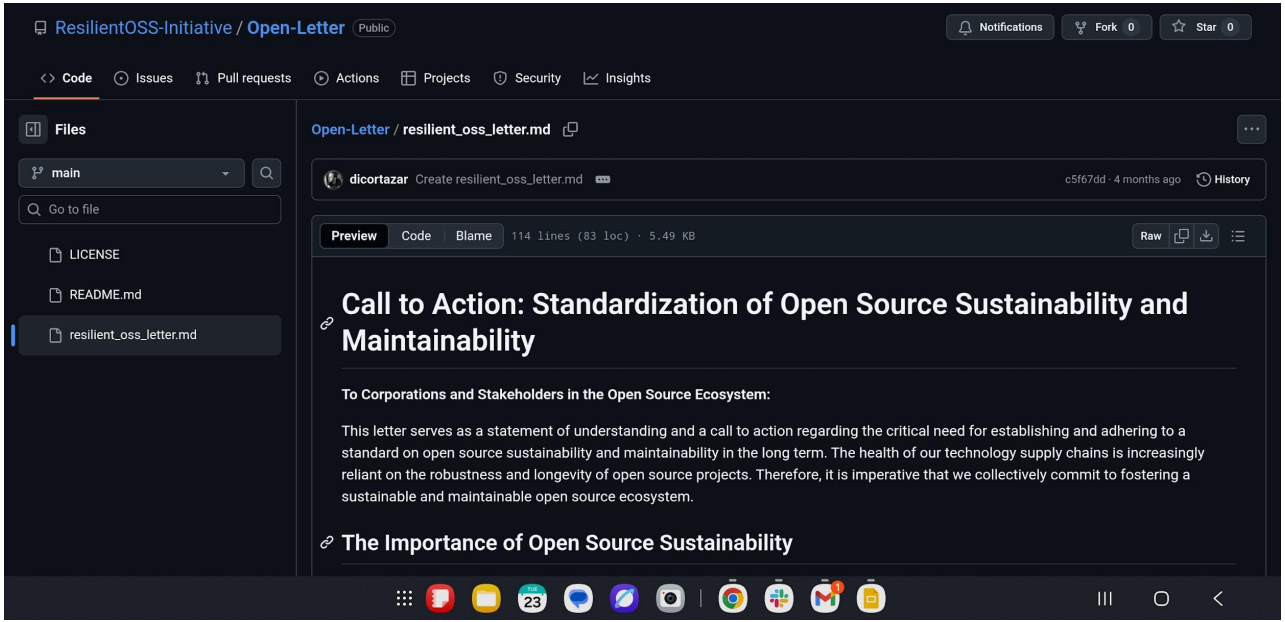
Export: Raw Formatted

1 2 3 4 5 ... 50 »

10

How can we approach this systematic problem?

Open Letter on OSS Sustainability



Journey

- OSS Compass Open Innovation Summit, Beijing
- **UN OSS Week, New York**
- OSS Summit, Amsterdam
- Digital Resilience Forum, Madrid

UN Open Source Week 2025

An Open Community for the Global Digital Compact

Date	16–20 June 2025
Venue	United Nations Headquarters, New York
Mode	In-person
Dress code	Business

Co-Hosts

United Nations Office for Digital and Emerging Technologies

United Nations Office of Information and Communications Technology

PwC Side Events Agenda

DPI | Digital Sovereignty & Resiliency | AI | Capacity Building | Global Priorities and SDGs

10:00 – 11:20	Session 1: The Indian DPI Experience – Building Interoperable, Society-Wide Infrastructure for the Public Good
11:20 – 11:40	Break
11:40 – 13:00	Session 2: Digital Public Goods – Building Inclusive DPI with Democratic Governance
13:00 – 14:00	Lunch
14:00 – 15:20	Session 3: Digital Public Infrastructure in the Global South – Innovation, Localisation, and Community Ownership
15:20 – 15:40	Break
15:40 – 17:00	Session 4: DPI Governance – Navigating Law, Ethics, and Safeguards in Digital Public Infrastructure
17:00	Event Close

United Nations

Journey

- OSS Compass Open Innovation Summit, Beijing
- UN OSS Week, New York
- **OSS Summit, Amsterdam**
- Digital Resilience Forum, Madrid

A key takeaway was the importance of a participatory approach. Any effort to define sustainability or risk must involve open-source projects themselves to avoid the perception of external parties (i.e., corporations) dictating terms. It was agreed that the goal isn't a single, rigid standard, but rather a set of guardrails or a taxonomy that empowers organizations to build their own risk approaches.

Next Steps

The group agreed to continue the conversation and move forward with the following actions:

- **Form a charter:** Draft a charter that outlines specific targets and work items for this effort.
- **Establish a communication channel:** A dedicated invite-only mailing list will be set up to facilitate ongoing discussion, at least initially.

We will share updates on these next steps as they develop and invite you to be as involved as you like. Thank you again for everyone's valuable contributions.

Journey

- OSS Compass Open Innovation Summit, Beijing
- UN OSS Week, New York
- OSS Summit, Amsterdam
- **Digital Resilience Forum, Madrid**

Eclipse Foundation
34.051 seguidores
5 días • Editado •

We're proud to be part of the Digital Resilience Forum on 29 October in Madrid. Join 300+ professionals and leaders working to shape resilient, diverse, and independent digital ecosystems.

Speakers include key figures from government, industry, and innovation:
· Omar Mohsine, OSS Coordinator, United Nations
· John Ellis, Codethink
· Adriana Groh, CEO, Sovereign Tech Agency
· Armando J. Manzueta Peña, Vice Minister of Public and Digital Innovation, Dominican Republic
· Juan Rico, Open Regulatory Compliance at Eclipse Foundation

🔗Join them! https://hubs.la/Q03Jt_vP0

#DigitalResilience #DRF2025 #innovation #opensource

traducción

Digital Resilience Forum

UN Development Goals: Making Digital Public Infrastructure more Resilient	Omar Mohsine, OSS Coordinator, United Nations
Why do you trust software?: A Journey for the Automotive Industry	John Ellis, President and Head of Product, Codethink
The Engine Room for Digital Sovereignty	Adriana Groh, CEO, Sovereign Tech Agency
Digital Sovereignty and Other Fables	Amanda Brock, CEO, OpenUK and Executive Producer State of Open Con








https://
digitalresilienceforum.com/

AboutCode Foundation
The not-for-profit AboutCode Foundation develops and advances open source code, data, and standards to empower users to automate and secure their software supply chains.

CEI-Sphere
CEI-Sphere is focused on empowering innovation in the Cloud-Edge-IoT (CEI) ecosystem. Its goal is to drive Large-Scale Pilots and support the development of an open, interoperable, and competitive ecosystem.

CHAOSS
CHAOSS is a Linux Foundation project focused on creating metrics, metrics models, and software to better understand open source community health on a global scale.

Drupal Association
The Drupal Association is the non-profit organization focused on accelerating Drupal, fostering the growth of the Drupal community.

The Eclipse Foundation
The Eclipse Foundation provides our global community of developers and 300+ member organisations with a business-friendly environment for open source software collaboration and innovation.

Linux Professional Institute
Linux Professional Institute (LPI) is the global certification standard and career support organization for open source professionals.

OpenForum Europe
OpenForum Europe is a not-for-profit, independent organisation dedicated to fostering an open, competitive European IT market and ensuring IT users have open, competitive choices.

Open Ireland Network
The Open Ireland Network is a not-for-profit social enterprise that enables Ireland's growing community of organisations and individuals across the island of Ireland who are passionate about all things open source.

The Open Logistics Foundation
The Open Logistics Foundation is a non-profit organisation that offers companies a neutral platform for the collaborative development of open source software.

OpenNebula Systems
OpenNebula is a powerful, but easy-to-use, open source platform for your enterprise's private, hybrid, or edge cloud infrastructure. OpenNebula unifies public cloud simplicity and agility with private cloud performance, security, and control.

OpenRail Association
The objective of the OpenRail Association initiative is to provide an open space to foster innovation and software development in the railway sector.

Open Source Conference Luxembourg
The conference that provides the opportunity to learn more about planned, ongoing and completed implementation of Open Source projects and platforms and to establish synergies with the people that have already worked through these upgrade processes.

OSPOlogy
OSPOlogy is a framework for organizations and local communities to use when organizing conferences related to open source management and OSPO setup. From Birds of a Feather to OSPO Tooling Workshops, templates are freely available for any organization to adopt at their events

TODO Group
TODO is an open community of practitioners with over 10 years of experience, whose mission is to identify key policy and process choices related to open source management and engagement within organizations, and to create educational materials that promote best practices

Sovereign Tech Agency
The Sovereign Tech Agency is the first publicly funded organization in Europe tasked with strengthening critical digital infrastructure. It identifies and invests in foundational open source software components and supports open technologies with broad societal importance. Providing digital services in the public interest enables the independent use of open technologies by the state, the private sector, organizations, and individuals, and safeguards security and technological diversity.

Digital Resilience Forum

International Initiatives to Grow Resilience

https://
digitalresilienceforum.com/

Moderator: Jennifer Tridgell

Main Auditorium

Panelists:

Armando J. Manzueta, Dominican Republic Government.

Cesar Martínez, Founding Partner, Intelligence Mill | Ph.D., The University of Texas at Austin.

Gina Plat, Interim Lead for the Open Source Program Office (OSPO) at the Ministry of the Interior and Kingdom Relations

Leonhard Kugler, Head Open Source Platform at ZenDiS

Moderator

Juan Rico, Senior Program Manager at Eclipse Foundation Europe

Main Auditorium

Panelists:

Philippe Ombredanne, Lead Maintainer of AboutCode

Stefano Zacchiroli, Co-founder and CSO (Chief Scientific Officer) of Software Heritage

Georg Link, Open Source Strategist and Director of Sales at Bitergia.

Darío García de Viedma, Fellow at the Elcano Royal Institute in the fields of technology and digital policy

Securing the Digital Supply Chain, a Practical Approach

Summarizing

- Sustainability / Health analysis are the third pillar together with license compliance and security vulnerabilities
- Incipient working group growing industrial practices (not affiliated with any foundation so far)
- You can **join the discussion in person** at the Digital Resilience Forum in Madrid on the 29th of October or
- You can **join the discussion in a virtual way**
    - Send an email to dizquierdo@bitergia.com

Bitergia