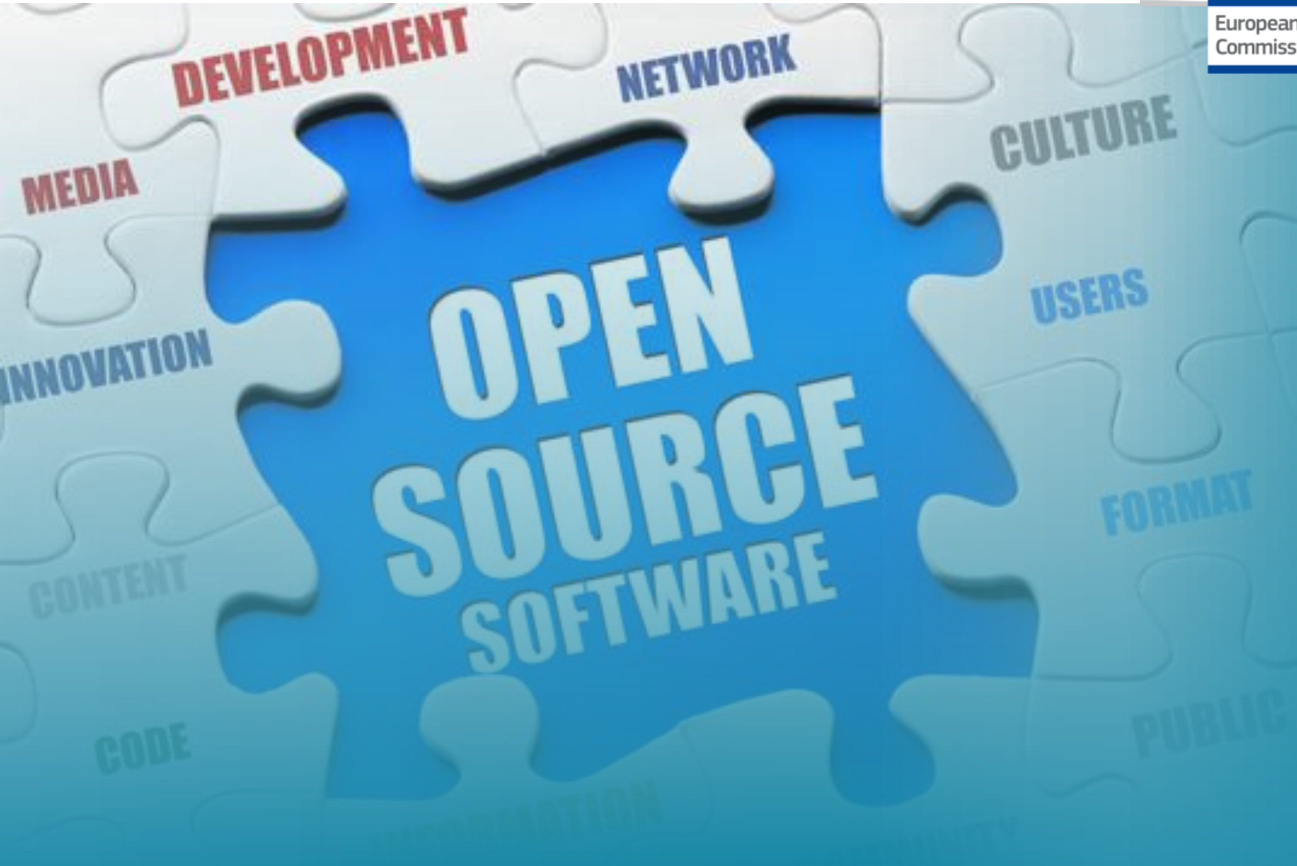
European Commission



EU-FOSSA 2: An EU initiative to tackle security of open source software

FOSS Policy Meetup
1 February 2019

ofe OpenForum Europe

fsfe

Marek Przybyszewski and Saranjit Arora
DIGIT Directorate-General for Informatics
European Commission

Agenda

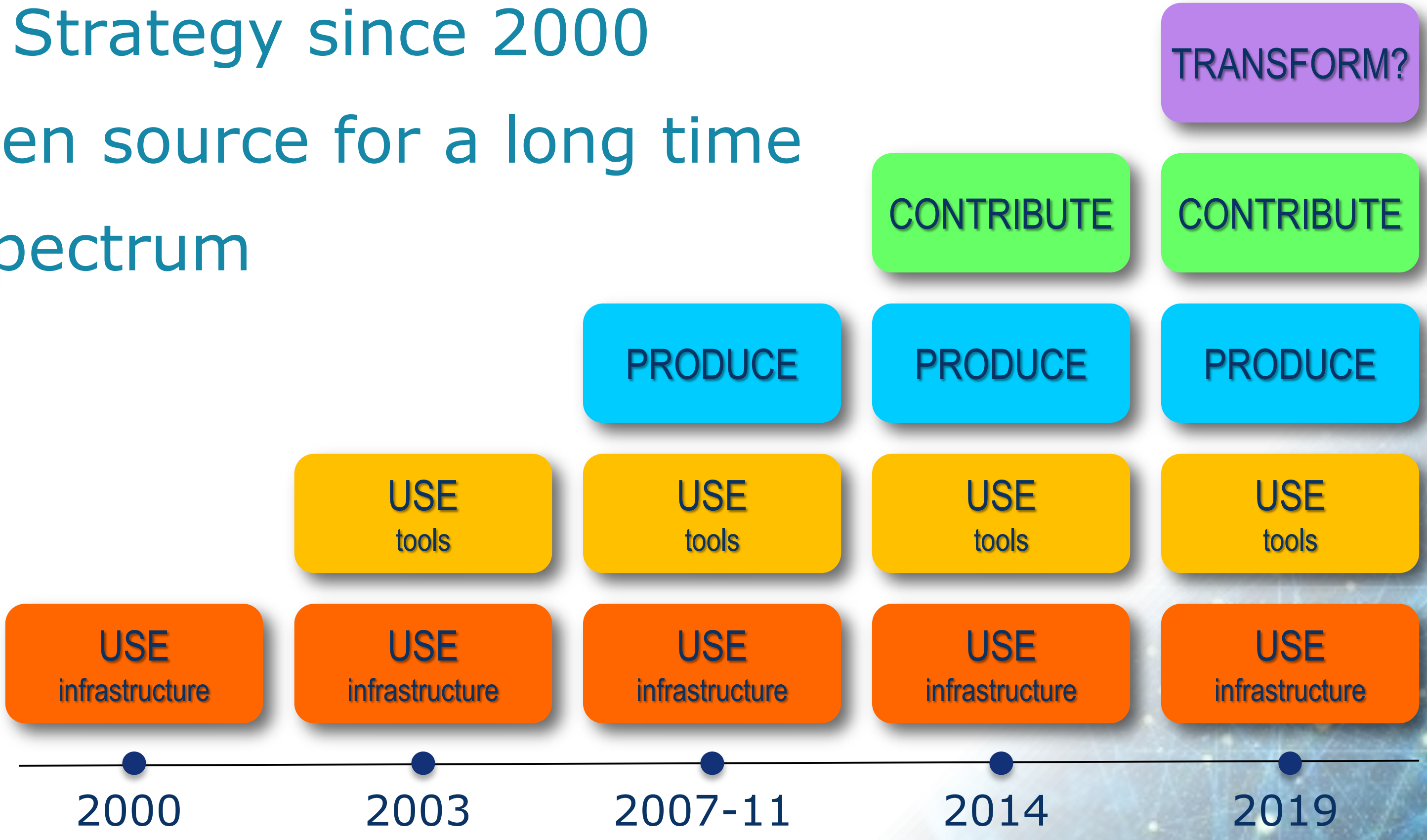
- Background
- EU-FOSSA Pilot → EU-FOSSA 2
- EU-FOSSA 2 – Progress to date

EU-FOSSA

Free and Open Source Software Auditing

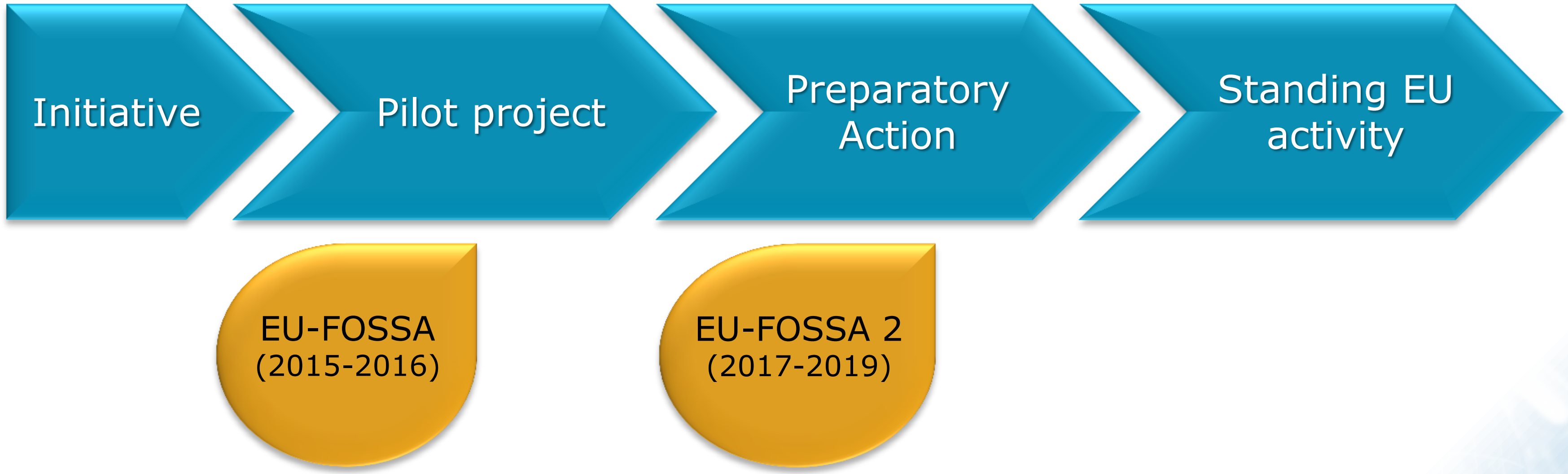
OSS @ the European Commission

- Open Source Software Strategy since 2000
- Enthusiastic user of open source for a long time
- OSS used across the spectrum
- Refresh in 2019



2000	2003	2007-11	2014	2019
				TRANSFORM?
			CONTRIBUTE	CONTRIBUTE
		PRODUCE	PRODUCE	PRODUCE
	USE tools	USE tools	USE tools	USE tools
USE infrastructure	USE infrastructure	USE infrastructure	USE infrastructure	USE infrastructure

EU-FOSSA journey



€500M+

European Parliament 1M€

European Parliament 2,6M€

EU-FOSSA - the Pilot project (2015-2016)

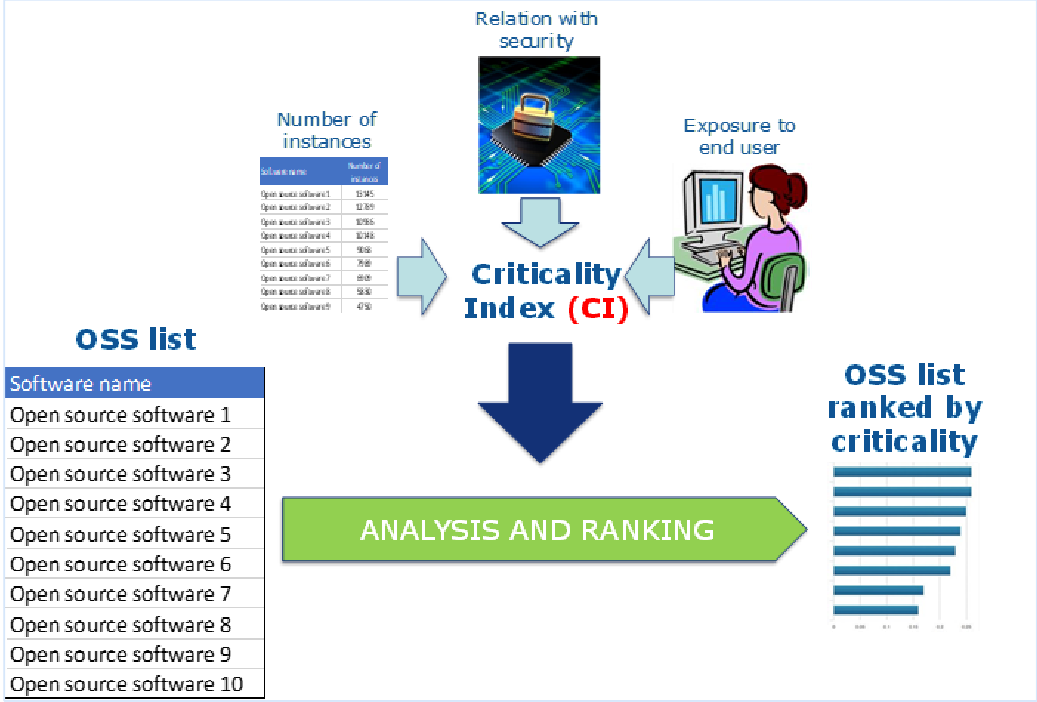
Approach

- Methodology
- Inventory of FOSS used at the EC
- Developer communities
- Public survey
- Formal code reviews

Lessons learned

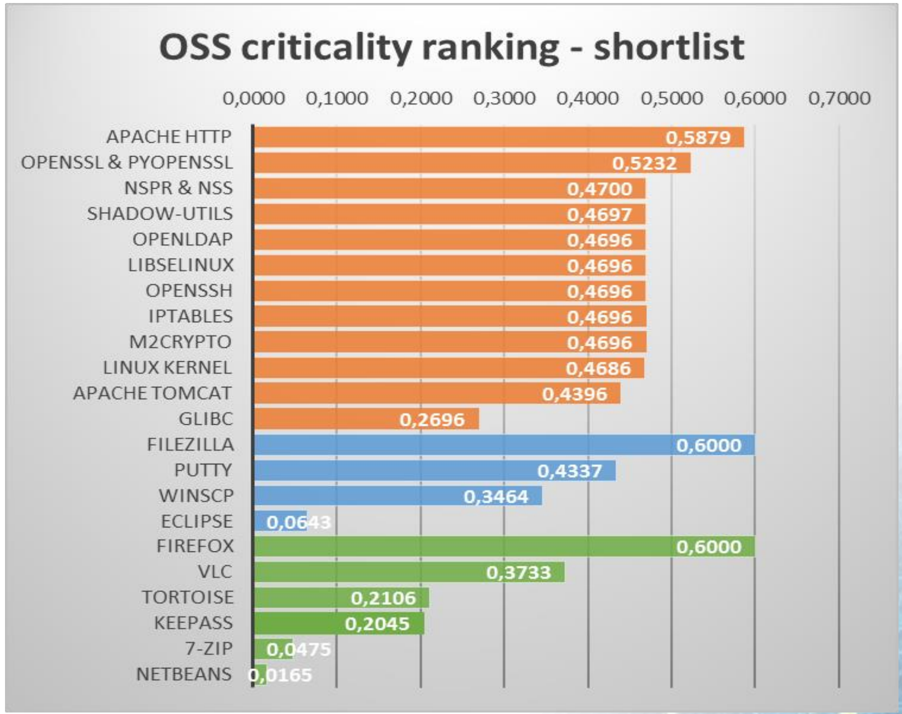
- Methodology works
- What about fixing bugs?
- Improve cooperation with communities
- Positive reaction
- Code reviews useful (but...)

EU-FOSSA - OSS criticality ranking


Relation with security
Number of instances
Software name
Number of instances
Open source software 1 15145
Open source software 2 12789
Open source software 3 10986
Open source software 4 10148
Open source software 5 9058
Open source software 6 7988
Open source software 7 6909
Open source software 8 5830
Open source software 9 4750
Exposure to end user
Criticality Index (CI)
OSS list ranked by criticality
ANALYSIS AND RANKING

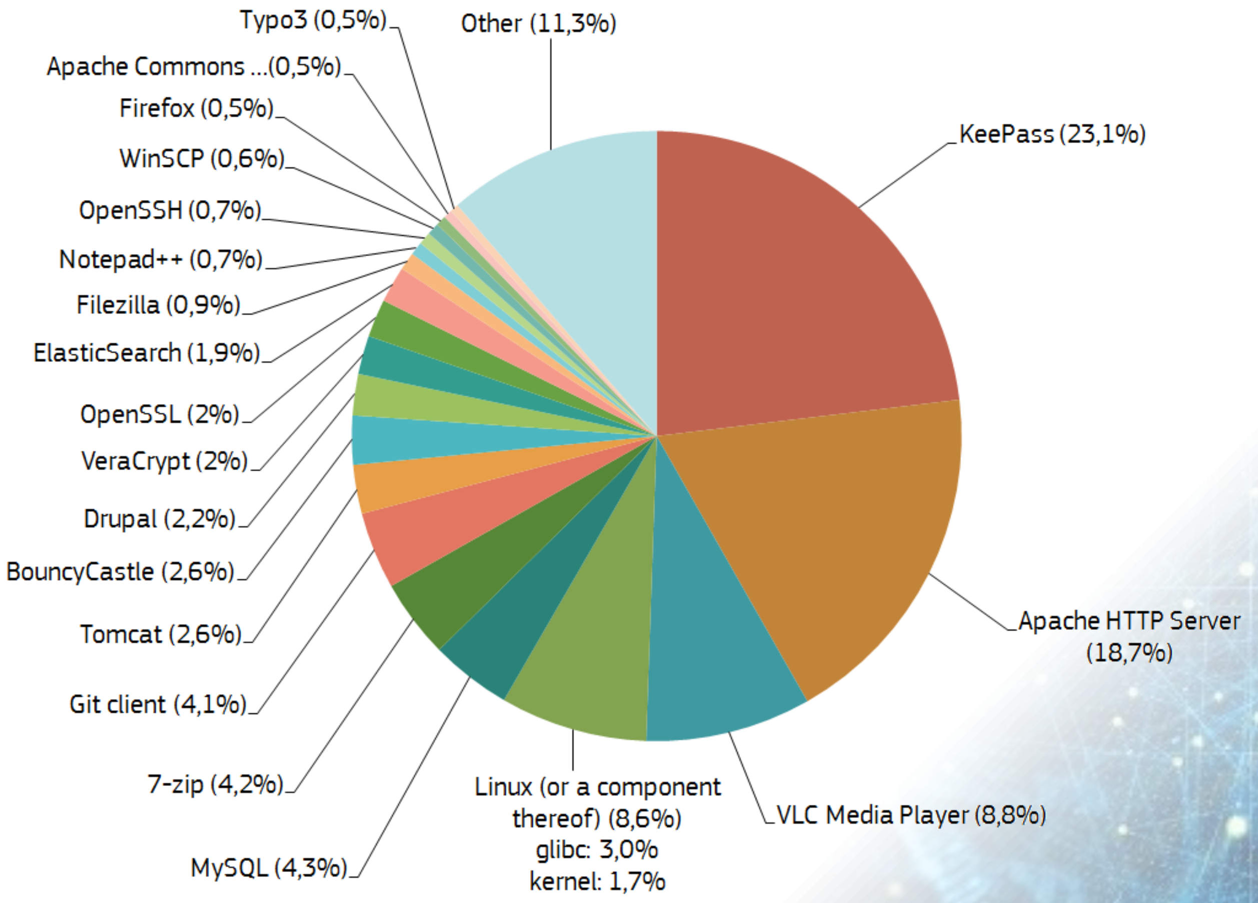
OSS list

Software name
Open source software 1
Open source software 2
Open source software 3
Open source software 4
Open source software 5
Open source software 6
Open source software 7
Open source software 8
Open source software 9
Open source software 10


OSS criticality ranking - shortlist

EU-FOSSA - public survey

- June 2016
- 3282 participants



EU-FOSSA 2 (2017-2019)

What is new?

- Increased scope
- Bug Bounties
- Hackathons
- Fixing already known bugs
- Closer cooperation with developer communities
- Improved communications programme

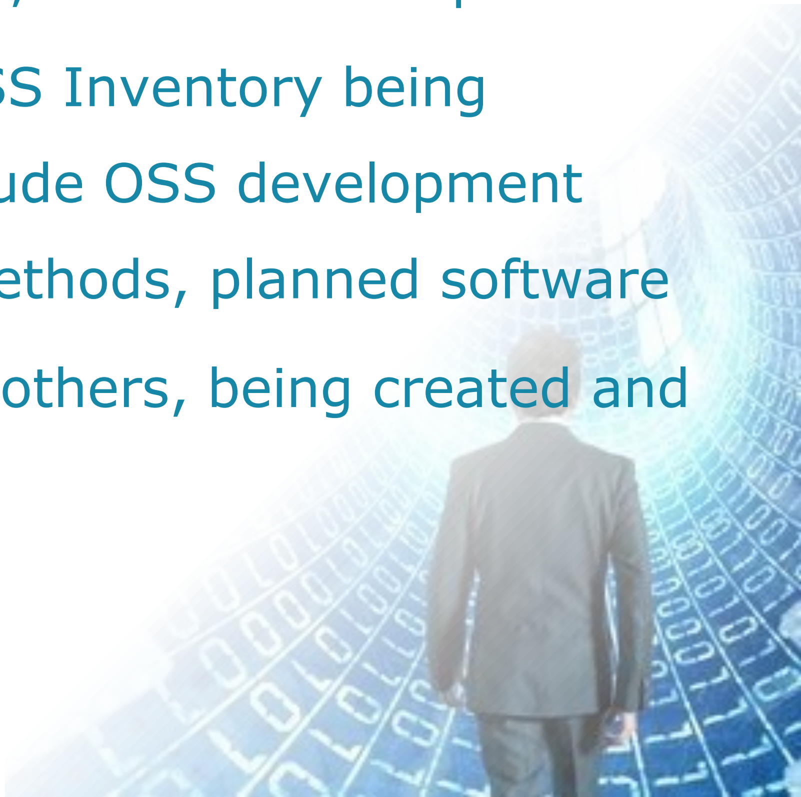
PLAN

Wider Scope

PROGRESS

- Expand scope beyond European Commission to other European institutions
- Include SDKs, frameworks, methods and *planned* OSS

- European Parliament, Council, EIB, EEAS, EES-COR, Council of Europe
- Commission OSS Inventory being updated to include OSS development frameworks, methods, planned software
- Inventories for others, being created and updated



PLAN

Bug Bounty programme

Proof of concept

- First time in EU institutions
- 28 active participants
- 6 weeks
- 6 bounties paid

Main programme

- ~15 activities
- Critical OSS used by EU institutions
- ~1 M€ budget
- Including high rewards

PROGRESS

Bug Bounties

- 3 vendors selected via public procurement tender (Intigriti/Deloitte → HackerOne → Econocom/YesWeHack)
- After consulting with European institutions and the last public survey, target software was identified and 15 contracts placed by end December 2018
- 12 Bug Bounties started in Jan 2019, 2 to start soon, with midPoint in March 2019

7-ZIP
Apache Kafka
Apache Tomcat
Drupal
DSS
FileZilla
FLUX TL
glibc
KeePass
midpoint
Notepad ++
PHP Symfony
PuTTY
VLC Media Player
WSO2

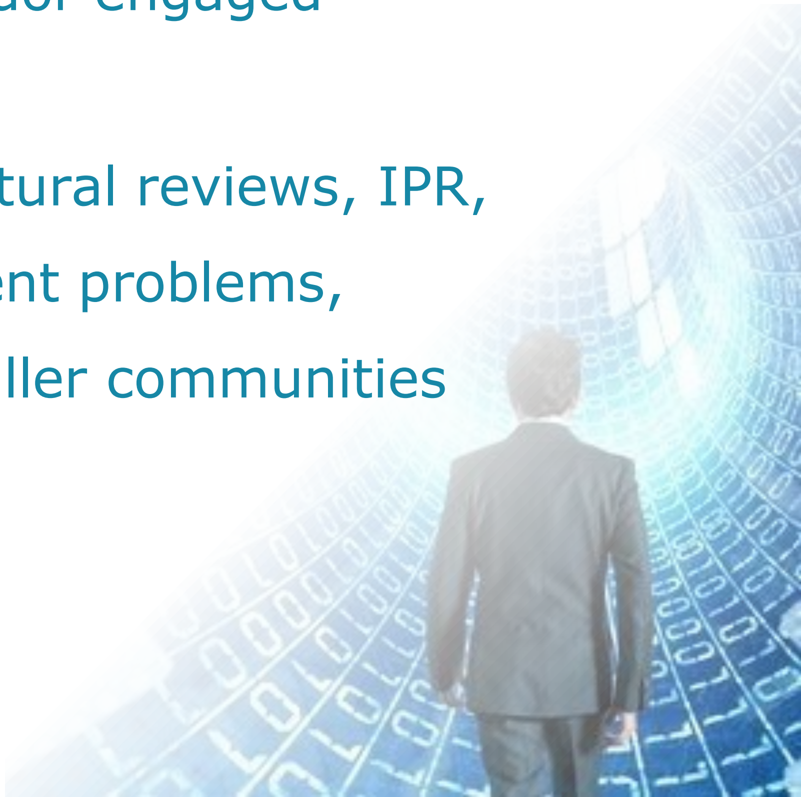
Hackathons

PLAN

- Plan 3 Hackathons (Brussels)
- Engage specialist Hackathon vendor
- Identify suitable projects
- Start planning

PROGRESS

- 6/7 April, 4/5 May, 5/6 Oct 2019
- Hackathon vendor engaged – BeMyApp, Paris
- Ideas: Architectural reviews, IPR, solving persistent problems, supporting smaller communities



European Commission

PLAN

PROGRESS

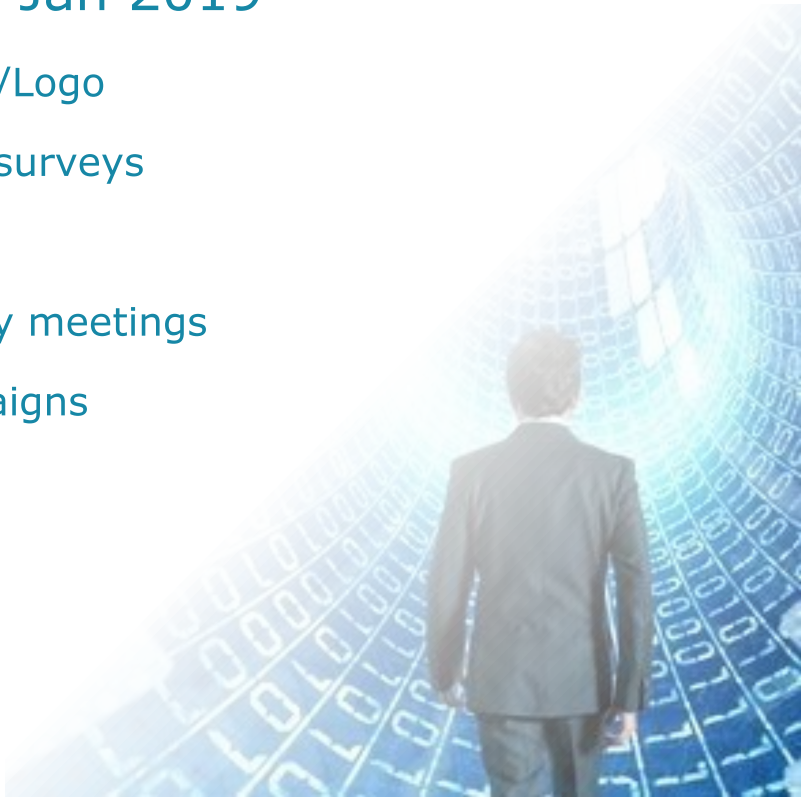
Communications

- Engage Communications

  Vendor, Internal coordinator
- Communicate with
  - OS Communities
  - EU Public

→

- For the Hackathons
- Work started in Jan 2019
  - Fresh Branding/Logo
  - Multiple public surveys
  - Conferences
  - OSS community meetings
  - Security Campaigns



EU-FOSSA 2 - the ultimate goal

- Improve security of open source software
- EU institutions working with open source software communities
- Make investment into the security of open source software a permanent action of the EU

European Commission

Thank you

Q | A

DIGIT-OSS-STRATEGY@ec.europa.eu