Open Source Compliance is the key to Community Interaction

my story

Oskar Swirtun

Founder and CEO

oskar.swirtun@fossid.com

FOSSID

1991

Linus starts the Linux kernel project

I just graduated from high school

FOSSID

2000

My first job after University

First telecom platform based on Linux

We use IBM for support of Linux

2001

First Open Source Directive that allows use of open source

And we start an education program within the company

IBM to spend 1 billion on Linux

IBM launches Eclipse foundation

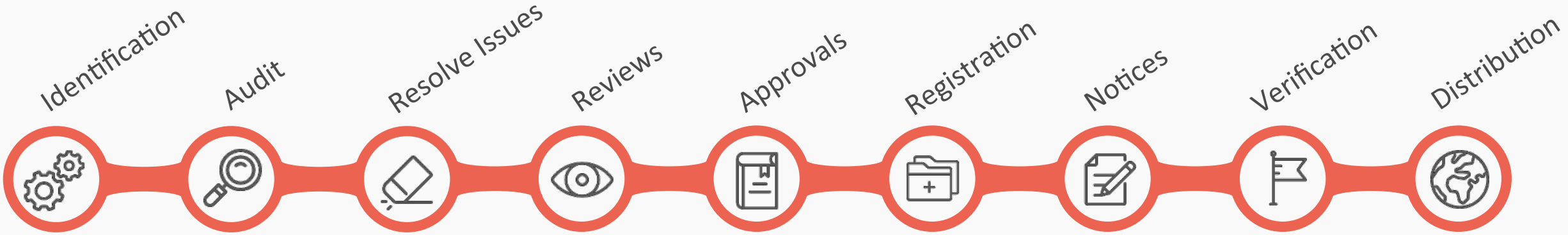
FOSSID

Consume

Distribute

Collaborate

FOSSID


Identification
Audit
Resolve Issues
Reviews
Approvals
Registration
Notices
Verification
Distribution

FOSSID

2003

SCO claims that there had been misappropriation of its UNIX System V code into Linux

Our CEO gets a letter from SCO, we are an old AT&T Unix licensee

Compliance is about legal risks

FOSSID

Compliance focus is on open source uncertainty and risks

- 95% of audits find unknown OSS
- 75% contain unknown licenses
- 50% of code audits contain GPL code

2005

Git is created by Linus

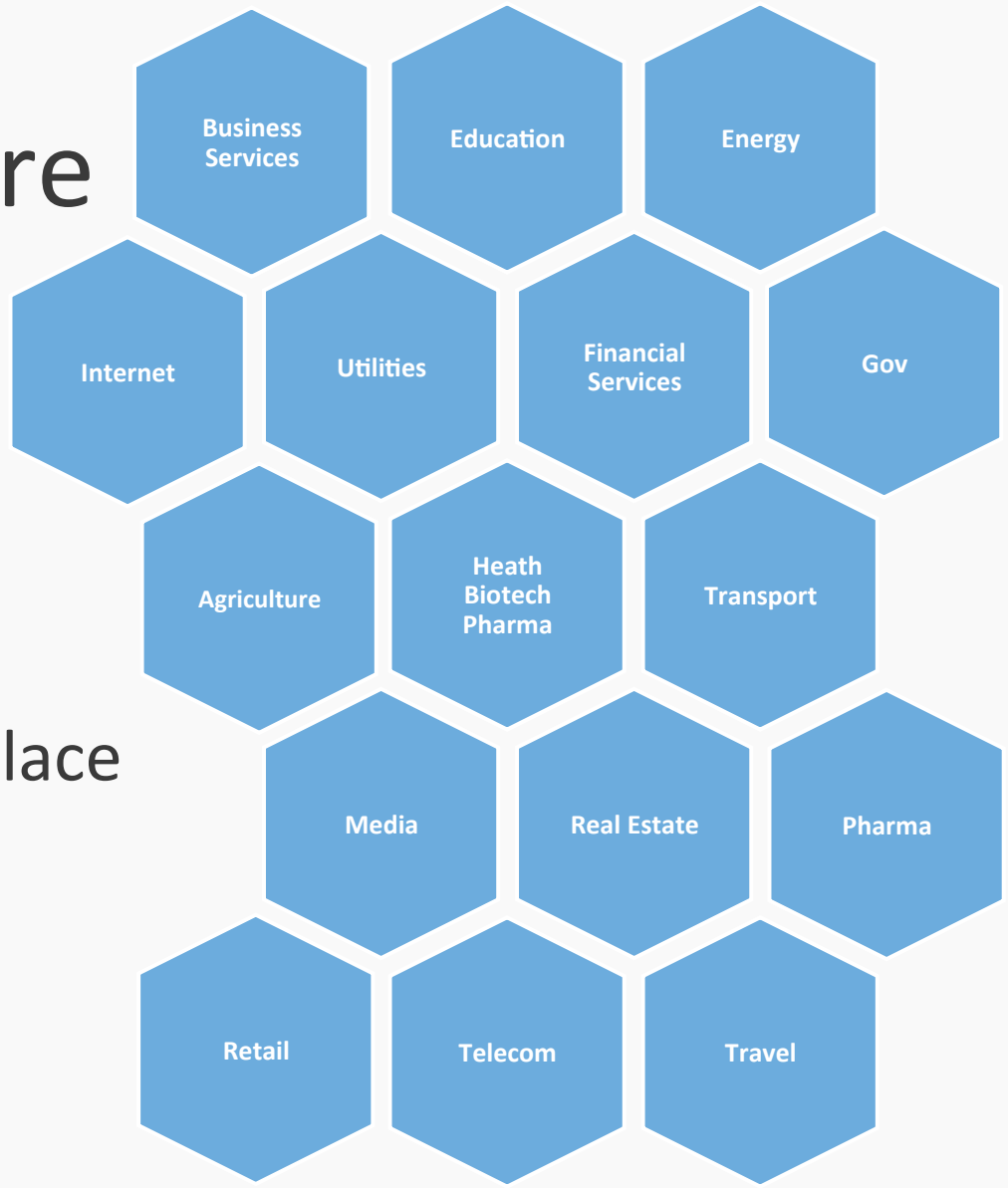
We acquire a large European telecom company

We see open source everywhere within the organization

FOSSID

Commoditization of software

- Open Source drives commoditization of software
- Commoditization is a sign of industry maturity
- Modular nature of a commodity marketplace accelerates innovation



FOSSID

2008

FOSSology is officially launched by HP

FOSSID

2011

We discover that 2/3 of all 3rd party software we use is open source

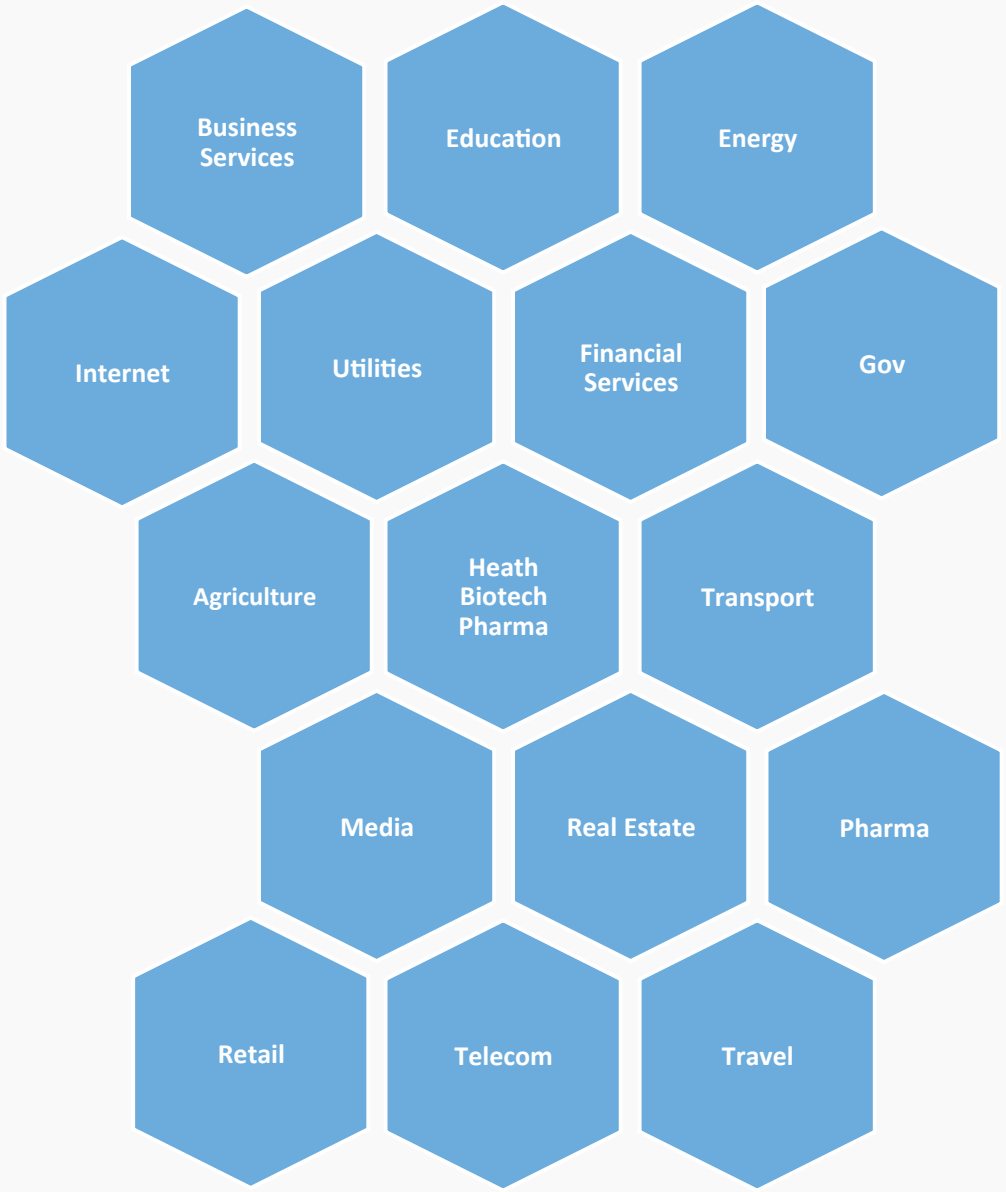
Android becomes the most popular smartphone operating system

Marc Andreessen writes “Why Software Is Eating The World” , The Wall Street Journal

FOSSID

Software runs the world

- Smartphone
- Robot trading
- Intelligent car
- Autonomous drones
- Smart medication



FOSSID

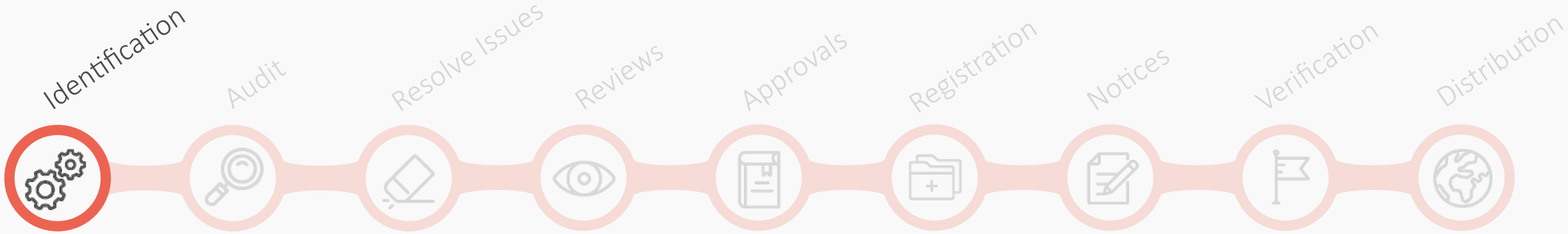
2014

Rachel King writes: “Open Source Eating Software World: Samsung”,
The Wall Street Journal

FOSSID

Compliance with focus on the opportunity

- Open Source is a catalyst in the transition of the old industries
  - More efficient software development
  - Standardisation of non differentiating software stack
  - High level of control over open source software

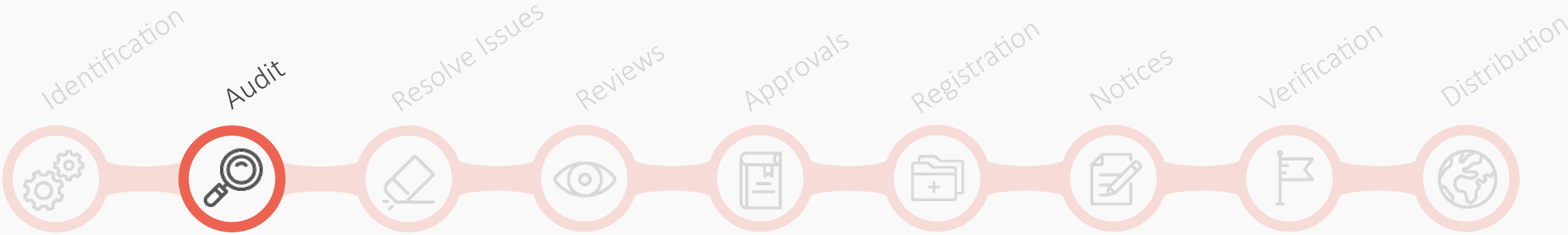


Identification

Monitor the entrance of open source in the company's software portfolio

1. Find: Engineers hate to write code that has already been written
2. Guide: Engineers need guidelines to make decisions about use of open source software
3. Understand: Engineers need means to quickly understand open source software origin, license requirements and risk

FOSSID

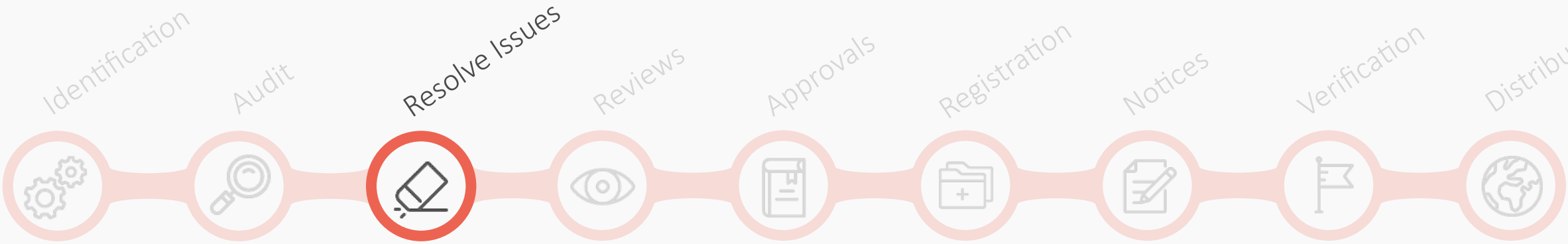


Audit

The second step in compliance due diligence consists of scanning the source code using automated analysis tools to discover matches with known open source projects.

1. Customized knowledge base: Encourage use of selected open source software base
2. Protect competitive advantage: Finding proprietary software in the open source product

FOSSID



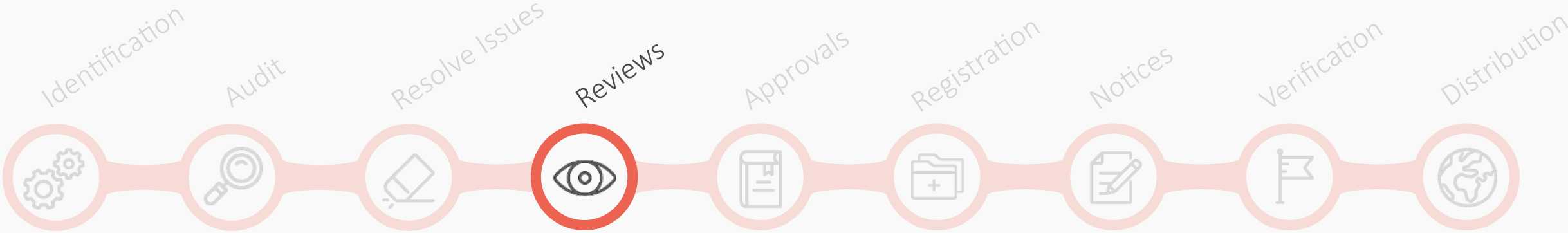
Resolve Issues

As a result of the audit step, detected issues (i.e. license conflicts) turn into tickets.

All tickets generated from the audit are monitored and tracked until they are closed.

Once all related tickets are closed, a new audit is performed to confirm that the issues are resolved.

FOSSID

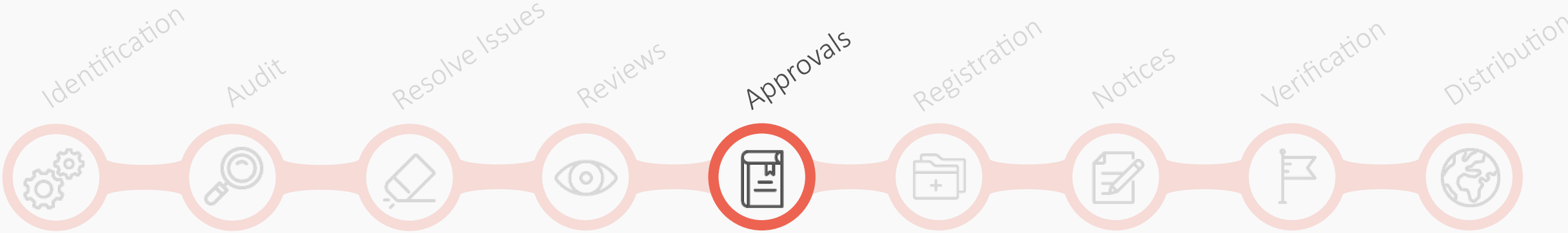


Reviews

Once all issues identified earlier are resolved, the compliance ticket is moved to the review process.

1. Architecture review: Analyse any interactions between the open source, 3rd party and proprietary code. The goal is to find out if the licensing obligations might extend from open source components to proprietary code
2. Linkage review: Find potentially problematic code combinations at the static and dynamic link level
3. Guidelines review: Ever changing open source landscape may need updates to company guidelines

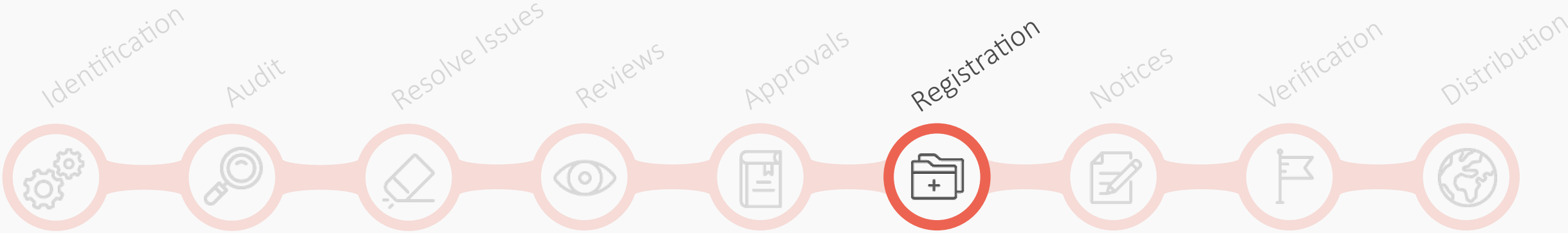
FOSSID



Approvals

Once all reviews have been completed, the software component’s compliance ticket moves to the approval step.

FOSSID

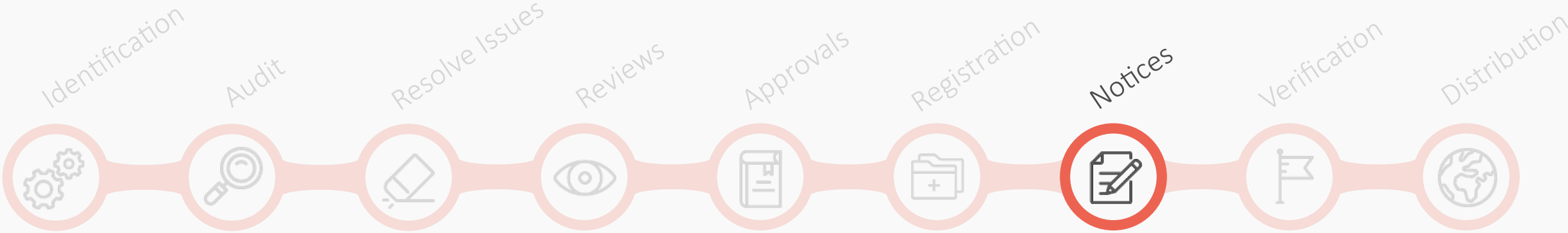


Registration

Once a software component has been approved for usage in a product, the following will take place:

1. It will be added to the software inventory that tracks open source use
2. The compliance ticket for the product in question will be updated to reflect the approval

FOSSID

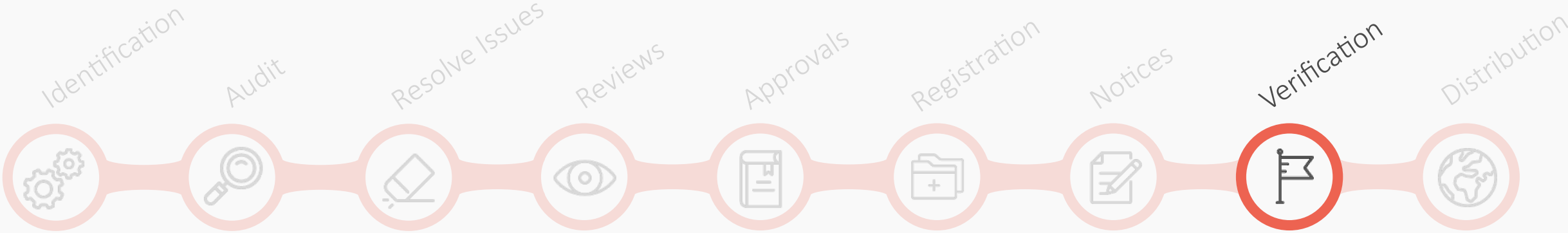


Notices

One of the key obligations when using open source is the documentation obligation, also referred to as the notice obligation

1. Acknowledge the use of open source by providing the required copyright and attribution notices
2. Reproduce the entire text of the license agreements for the open source code included in the product
3. Inform the end user how to obtain a copy of the source code (when applicable)

FOSSID

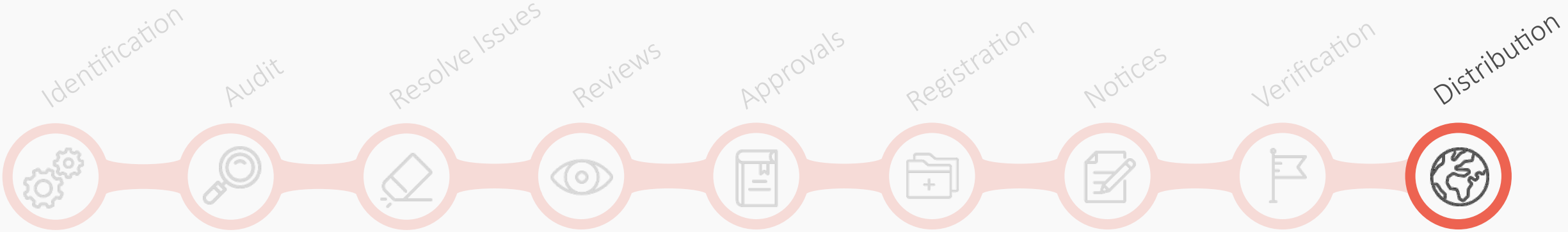


Verification

The goal of this step is to ensure that:

1. All open source packages destined for distribution have been identified and approved
2. Source code packages (including modifications) have been verified to match the binary equivalent being shipped with the product
3. Appropriate notices have been included in the product documentation with regard to attribution and to inform end-users of their right to request code (when applicable)
4. All source code has been reviewed and approved to be distributed externally

FOSSID



Distribution

Once the verification step is completed, it's time to decide the distribution mechanism:

1. Distribution website: upload the open source packages to the distribution website: labeled with the product and version it corresponds to.
2. Written offer

FOSSID

2016

Open source is again challenged by Copyright Trolls

Using open source is no longer a choice

FOSSID

FOSSID

Open Source Today

Rapid Expansion

Collaborative software is growing at the speed of light

1 **project** created every **second** in GitHub

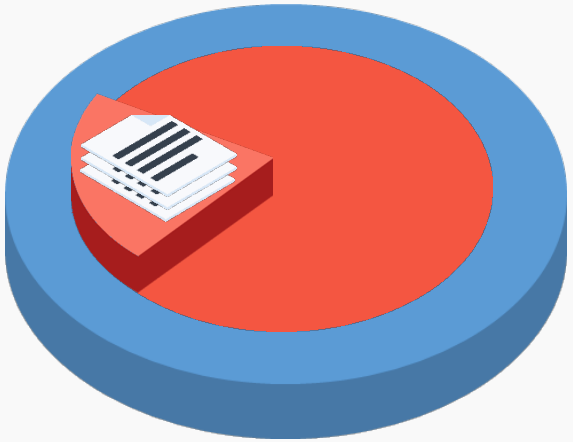
Growing Adoption

Open Source is **the foundation** for **nearly all** software applications

Today **programmers** are as likely to **use open source** as they are to write their own

License Absence

Most of the open source projects out there lack license information



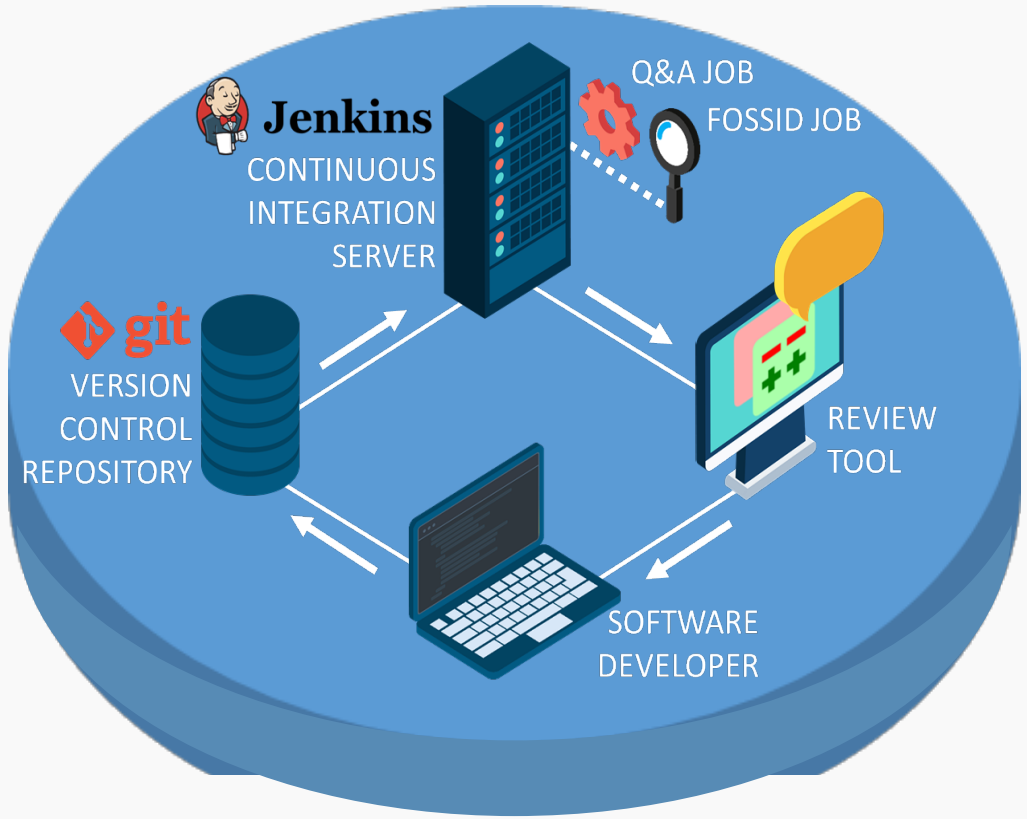
Less than 20% of projects in GitHub **have a license**

Linux Foundation

- Companies must master open source if they want to master software
- Compliance is the key to mastering open source
  - Consumption
  - Contribution
  - Collaboration

Compliance needs to be automated

- Transparent part of the development
- Integral part of the development process
- Encourage and not hinder re-use



FOSSID

2017…

The main purpose for a Compliance Process is to help to choose the right open source

- not find the wrong ones

- Coming from corporate environment we want to :
  - Compliance is an engineering tool
  - Compliance is up to date with continuously updated database
  - Compliance is flexible, with different rules and choices dependent on a user
  - Compliance is precise with no fault positives
  - Compliance is sharing with open source compliance projects like FOSSology

FOSSID

Companies must master and be ~~open source~~ compliance leaders if they are to become software leaders

www.fossid.com

Open Source Compliance is the key to Community Interaction

Software is in the center of growth for all technology companies today. Whether it's an automotive company trying to build an autonomous car or just optimizing the performance of their combustion engine, a telecom company, a cloud provider, a finance institution, or any other technology company, they all need to become software authorities.

Software development is to a large extent about re-use of code and successful technology companies need to master open source which is the main source of software components today. But success is also about being able to protect the ideas and the companies' specific domain expertise.

To re-use and share software may be contradictory to protecting proprietary software assets and that contradiction defines the importance of compliance in any technology company. Open source compliance is the key to consumption, contributions and to successful community interaction. Once the development strategy, policies and directives are defined, compliance is all about implementation.

It's not about policing the engineers; it is about enabling engineers to securely tap into the vast open source software resources available in order to create the most efficient software development organizations in their respective technology domains.

In this talk, Oskar Swirtun (Founder and CEO of FOSSID) will discuss the problems enterprises face when it comes to implementing successful open source software strategies and will explore various compliance flows that will enable enterprises to have faster and more effective development, better community interaction, and lasting differentiation for technology companies.

FOSSID