



# OPEN SOURCE DILIGENCE: FROM RISK ASSESSMENT TO POST-CLOSE INTEGRATION

Jari Koivisto

2024-11-25

# SPEAKER



**Jari Koivisto**  
Open Source Specialist

# AGENDA

- 1 Open Source Due Diligence (OSDD)
  - Why it is important for M&A
- 2 Open Source Due Diligence in practice
- 3 OSDD Specialists' role at post-close
- 4 Summary

# OPEN SOURCE DUE DILIGENCE

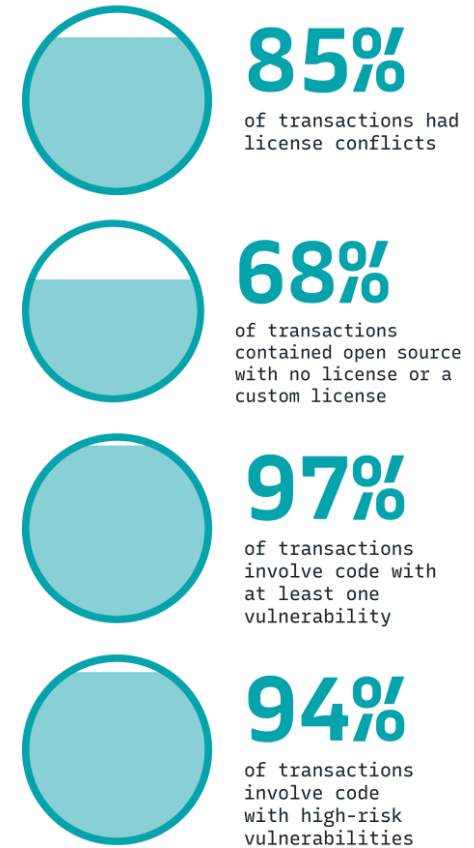
What is OSDD and why it is important for M&A



# OPEN SOURCE DUE DILIGENCE IS IMPORTANT FOR TECH M&A

## Software development and risk today

- Today 70-90% of code bases are Open Source Software, see e.g. [Synopsys' 2024 Open Source Risk in M&A by the Numbers](#) report for details
  - Many potential Target companies do not manage OSS well → unknown risks in M&A
    - Open Source disclosure lists that Targets provide are normally far from complete
- All Open Source code has potential licensing and cyber security risks
  - **Licensing risk:** Target's IP may be at risk – once integrated even the Buyer's IP may be at risk
  - **Cyber security risk:** Data breaches and ransomware attacks can be very expensive



Source: 2024 Open Source Risk in M&A by the Numbers, Synopsys whitepaper

# OPEN SOURCE DUE DILIGENCE IS IMPORTANT FOR TECH M&A

Informs the deal and future plans

- Identify if there are any major surprises
- However, it is less about stopping the deals – but that can happen too, if risks and/or mitigation costs are too high
  - Many critical/major Open Source issues may also affect deal terms and even valuation
- Estimate how much time and money is needed to mitigate issues and integrate
- High criticality risks are often mitigated before the deal closes



# Identifying Issues

## Licensing risks

- OSS Licenses have obligations that one needs to fulfill
  - Even permissive licenses
- Components without license
  - E.g. Target: ***"We did not find any license, so we assumed that the code was public domain."***

## Security risks

- Are there known vulnerabilities (CVEs)
- According to **2024 Open Source Risk in M&A by the Numbers:**
  - 97% of transactions contained at least one vulnerability, mean 439 vulnerabilities per transaction
  - 94% of transactions involve code with high-risk vulnerabilities
- Exploitable or not?
  - E.g. vulnerable only if used in 32-bit platform and Target only uses 64-bit platforms
- Does Target have processes to identify and remediate security issues?

## Open Source Due Diligence for M&A

## Buyer to know what they are buying

- Without a good Open Source DD, Buyer may spend millions/billions on something that they need to open source
  - E.g. OpenWrt
- Is the price correct?

## Buyer to understand what it takes to mitigate issues

- Validating Roadmap
- High-risk issues → closing conditions
  - E.g. embedded copyleft code

Confirming Value

Planning

# OPEN SOURCE DUE DILIGENCE IN PRACTICE

A tested process of how to execute OSDD for M&A





# OPEN SOURCE DUE DILIGENCE

## Execution Approaches

### Questionnaires and meetings

- The goal is to find out how and how well OSS component use is managed

### Source code audit

- The goal is to get an understanding of the risk level
  - Licensing risk
  - Cyber security risk
- Verify how effective the OSS management is
  - Target may have an excellent OSS Policy and training on paper, but if not put into use, those have no value
  - Are the codebase findings in line with the questionnaire answers?

# PREPARE BEFORE THE ACTUAL DUE DILIGENCE WORK STARTS

Successful DD requires good preparation

- Early enough:
  - Prepare questionnaire(s) and checklist(s)
  - Select the 3<sup>rd</sup> party auditor, agree on business terms
  - Agree on who is the contact point for the Target
    - Target personnel will be very busy and having a single person contact makes their life easier
- Once the Target is known:
  - Study Target's offering
  - Business Unit's plans

# OPEN SOURCE DUE DILIGENCE

## Timeline

### Scoping

Open Source Due Diligence will take time. Agree on what products and versions need to be audited.

### Planning and Priority

Review issues, prioritize and create remediation plans. Critical issues remediated normally pre-close.

### Negotiate

Be prepared to negotiate.  
Buyer to reassess deal terms.

# OPEN SOURCE DUE DILIGENCE

## Process observations

- Buyer wants to understand Target's:
    - Open Source policies and processes
    - Traditionally Open Source license compliance was the main focus
    - Today additional focus on Open Source management processes and Open Source vulnerabilities
  - Buyer does not have access to the source code
    - Buyer does not want to see the source code
    - Target does not want to share their source code
- } 3<sup>rd</sup> party auditor often the answer
- In the end Open Source Due Diligence produces
    - Open Source risk report
    - Mitigation plan, which includes estimates of cost (time / money)

# OPEN SOURCE POLICIES AND PROCESSES

Buyer to examine the quality of Target's Open Source policies and processes

- Normally not much time → the quickest way is to use a questionnaire and a meeting with Target
- Buyer should also request a disclosure list (SBOM) of all 3<sup>rd</sup> party components
  - Good indicator of Target's processes
    - E.g. once the disclosure list had 7 items and the code base was pretty large and the code audit found over 1,000 components and snippets
- Tips:
  - Keep the questionnaire as short as possible, but include all relevant and important questions
  - There are publicly available checklists that can be used as a starting point for the questionnaire(s)
  - Send the questionnaire to Target as soon as possible and give them a couple of days to answer

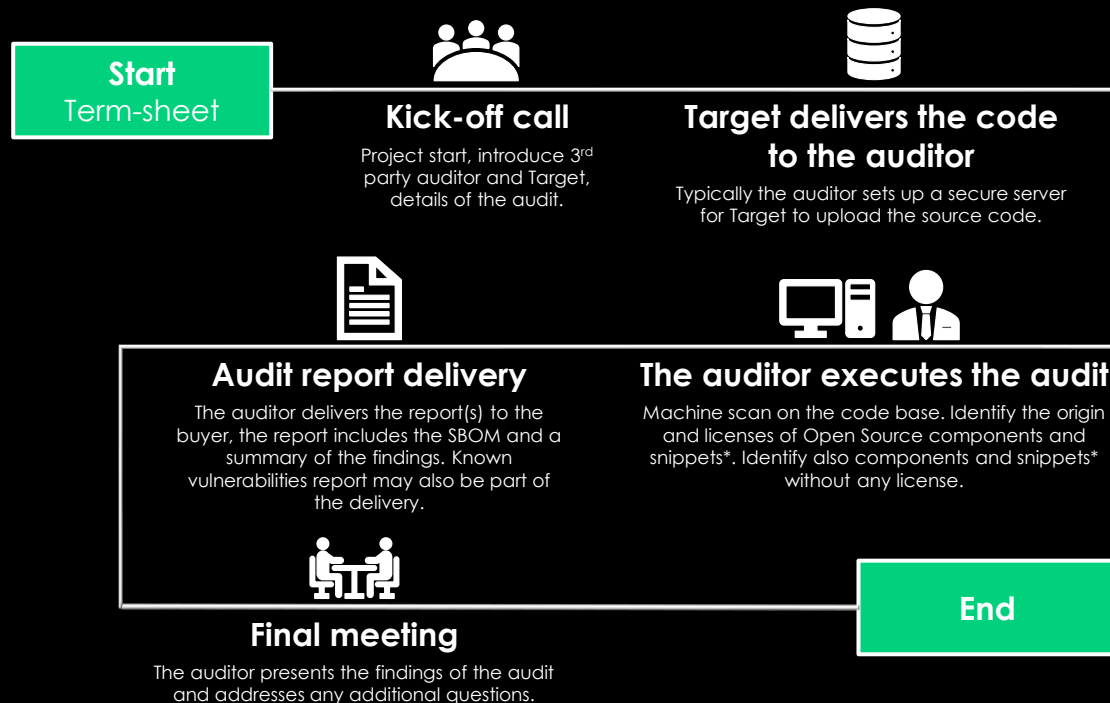
# WHAT SHOULD BE EXPLORED

Based on the questionnaire(s) and meetings with Target

- Does Target have a written Open Source Policy?
  - If yes, how it compares to Buyer's Open Source Policy
  - Policies and processes for OSS use and contributing back to the OSS Projects
- Does Target have an Open Source Compliance Program, OSPO, OSRB?
- Policies and processes handling known vulnerabilities (CVEs)
- Policies and processes for out-of-support or deprecated OSS components
- What tools Target uses
  - SCA, SBOMs management, vulnerabilities management
- OpenChain certified?
  - ISO 5230 conformant? and/or ISO 18974 conformant?



# SOURCE CODE AUDIT USING 3<sup>RD</sup> PARTY AUDITOR



- Typically, Target's source codes delivered to the auditor
- Auditor can also go to Target's site or have a proxy laptop there
- Snippet-level audit recommended
  - Copyleft snippets in Target's IP
    - E.g. CC-BY-SA snippets from StackOverflow very common
  - GPL and other copyleft snippets also possible
- AI-generated code snippets need to be properly handled too
  - Copyrights, attributions, license texts?
  - Copyleft?

\* Snippet level scan & audit recommended

# EXPECTATIONS

## **Start-up (typical Target):**

- May not have written Open Source Policy, but likely have processes to accept/reject Open Source components, e.g. ask the CTO
- Maybe a code scan before the due diligence as part of the preparation, but often scans are not part of the workflow
- Audit findings:
  - A lot of findings, but mostly permissive licenses
  - Also CC-BY-SA licensed snippets
  - CVEs, (outdated components)

## **Mature company:**

- Open Source Policy and processes in place
- License compliance is taken care of, some may even have a virtual OSPO or OSPO
- Audit findings:
  - Always something → Target often proactively remediates
  - CC-BY-SA licensed snippets
  - CVEs, outdated components

# OPEN SOURCE DUE DILIGENCE PRODUCES REPORTS AND REMEDIATION PLANS

- OSS License compliance issues report
- OSS Security issues report
  - Possibly part of the overall Security Due Diligence Audit report
- Remediation Plan(s)
  - How to remediate OSS license compliance issues
  - How to remediate current OSS known vulnerabilities
  - (Processes improvement plans)
  - (Target OSS training plans)
- Issues remediation planning: Target knows the code the best → keep them in the loop and ask for suggestions and timelines

Remove	Renew
Replace	Relicense
Rewrite	Respect

# TAKING ADVANTAGE OF THE OPEN SOURCE DUE DILIGENCE RESULTS POST-CLOSE

The ones who executed the OSDD have the best knowledge



# ACQUISITION INTEGRATION

Depending on the Integration scenario

- Acquisition Integration starts after the deal closes
- At the beginning the Acquisition Integration people have limited knowledge of the Target
- People who conducted the Open Source Due Diligence and produced the reports and remediation plans have the latest information
- Things to consider:
  - Do **not** throw the Open Source Due Diligence reports and remediation plans over the fence to Acquisition Integration and hope for the best
  - A good practice is that people who conducted the Open Source Due Diligence help the Acquisition Integration and Business Unit at least at the beginning of the Integration phase
  - OSDD specialists to participate in the first integration meetings
    - Sometimes just 1-2 meetings are needed, sometimes several meetings over the months are needed

# ACQUISITION INTEGRATION

## Open Source Due Diligence specialists' role

- Go through the Open Source Due Diligence audit report(s):
  - Explain the issues and suggested remediation actions
    - Issues may be in OSS Licensing, OSS vulnerabilities, processes, etc.
  - Answer any questions (Business Unit, OSPO/BU Legal, Acquisition Integration)
- New information acquired
  - During the first weeks and months of Integration more info is gathered
  - Some remediation recommendations need adjusting or possibly some issues are no longer issues
    - Open Source DD specialist can help the Acquisition Integration Team and Business Unit
- Business Unit plans changed?
  - In case BU changes the plans post-close → Open Source Issues may be different
    - E.g. SaaS solution → Shipped solution



# SUMMARY



# SUMMARY

- Open Source Due Diligence very important for M&A
- Prepare all questionnaires and select 3<sup>rd</sup> party auditor well in advance
- Two main tracks in OSDD:
  1. Questionnaire(s) and meetings
  2. Source code audit (by 3<sup>rd</sup> party auditor)
- Open Source practices and processes analysis
- Source code audit: Licensing and Security risks analysis
- Cost (time / money) of issues remediation
- People who conducted OSDD to participate in Acquisition Integration
  - A meeting or two and if needed for longer



# Questions and answers

# Jari Koivisto

- [jari.p.koivisto@iki.fi](mailto:jari.p.koivisto@iki.fi)
- <https://www.linkedin.com/in/jarikoivisto/>
- <https://github.com/winterrocks/>

## CONTACT INFO



[LinkedIn/in/jarikoivisto](https://www.linkedin.com/in/jarikoivisto/)

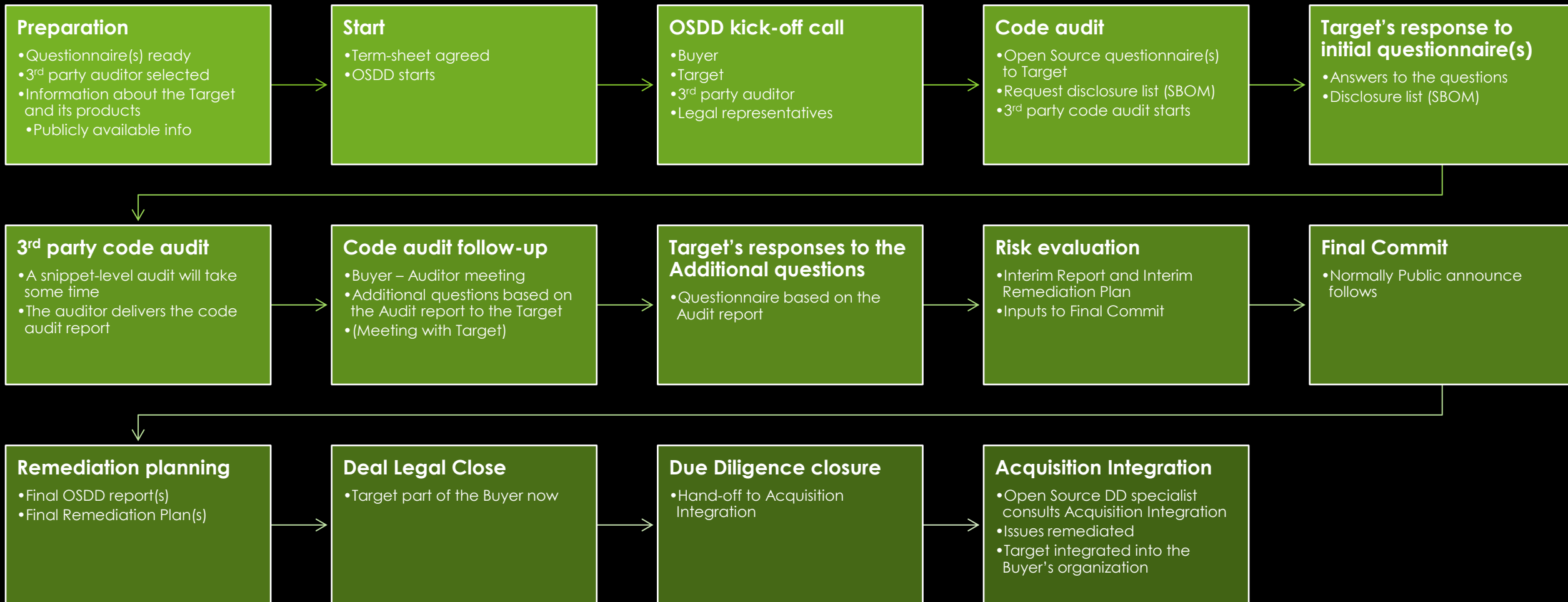
# BACKUP SLIDES

Some additional slides that can be useful



# OPEN SOURCE DUE DILIGENCE PROCESS

An example of how the whole process may look like





# WHAT IF FULL OPEN SOURCE DUE DILIGENCE CANNOT BE DONE PRIOR DEAL CLOSE?

- No time to do full OSDD prior to the deal's Legal Close?
- Continue the audit post-close
- Options to have:
  - Escrow
  - Reps/Warranties
    - Nowadays more insurers in this space