

# Open Data **Standards** for Open Source Software Risk Management **Routines**: An Examination of SPDX

1

**Georg Link**

*Coauthors:* **Robin Gandhi** and **Matt Germonprez**

GROUP 2018, Sanibel Island, Florida, USA



# SPDX Community

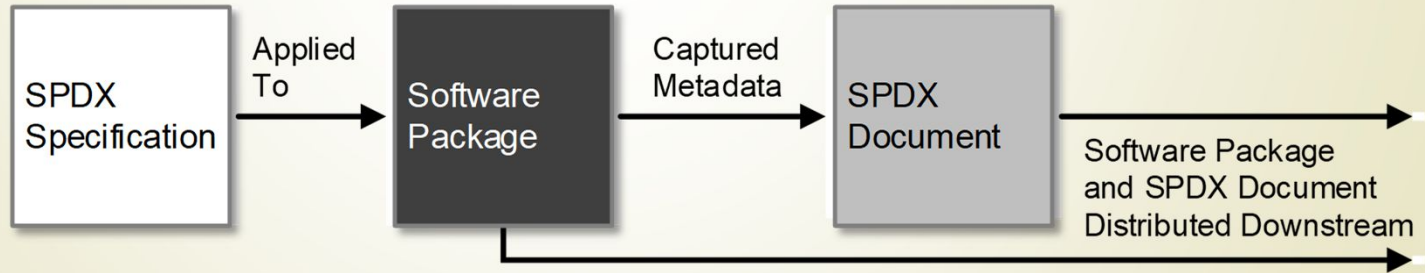


- SPDX® (Software Package Data Exchange®)
- The vision of SPDX is to achieve license compliance with minimal cost across the supply chain
- SPDX community produces
  - License List
  - SPDX specification
  - Tools



# The SPDX Specification

- ▶ “The Software Package Data Exchange® (SPDX®) specification is a **standard format** for communicating the components, licenses and copyrights associated with software packages.” - [www.spdx.org](http://www.spdx.org)





# Research Questions

- ▶ RQ1: *How do organizations participating in the SPDX community describe their **local interpretations** of communally structured OSS risk management routines?*



# Research Questions

- RQ1: *How do organizations participating in the SPDX community describe their **local interpretations** of communally structured OSS risk management routines?*
- RQ2: *How do these local interpretations influence the extent of their SPDX **adoption**?*



# Research Questions

- RQ1: *How do organizations participating in the SPDX community describe their **local interpretations** of communally structured OSS risk management routines?*
- RQ2: *How do these local interpretations influence the extent of their SPDX **adoption**?*
- RQ3: *How do these member organizations seek to guide the **advancement** of the shared SPDX specification?*



7

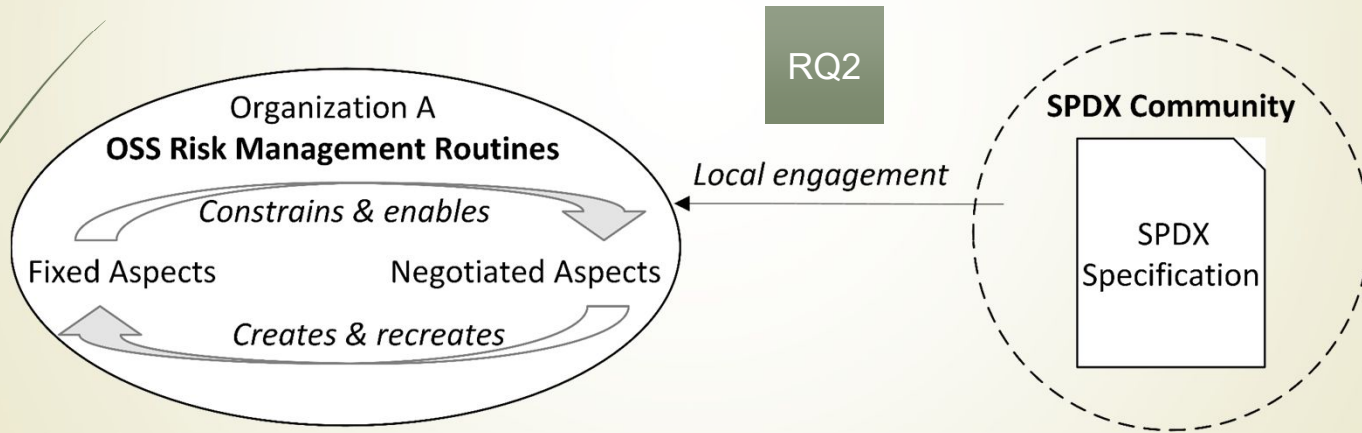
# Shared OSS Risk Management Routines In the Shared SPDX Standard Development





8

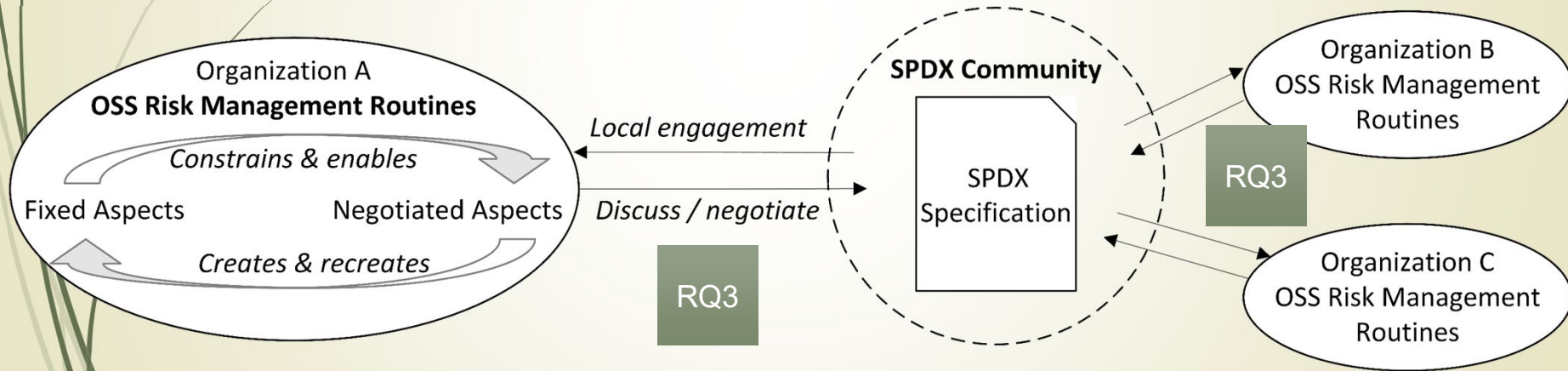
# Shared OSS Risk Management Routines In the Shared SPDX Standard Development







# Shared OSS Risk Management Routines In the Shared SPDX Standard Development



# Data Collection and Validation

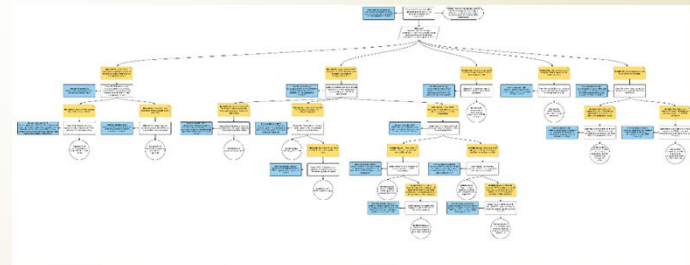
## Assurance Case Method

- 16 Interviews
- 15 Organizations
- 10 hours of recording
- Field notes

## Validation

- Focus Group with 15 SPDX members at Open Source Leadership Summit 2017

Interview Protocol	
SPDX Case Study IRB Approved: #473-16-EX	
Main Interview Question: In the context of software exchange, could you describe your organization's OSS risk management routines?	
Follow-up questions:	
Sense Making	Q1: How did your organization become familiar with or adopt SPDX?
Adoption Strategies	Q1.1: Can you speak about SPDX adoption strategies in your organization and how those strategies have been informed (i.e., through the SPDX website, discussions in the SPDX community, upstream and downstream vendors, or elsewhere)?
SPDX Use Cases	Q1.2: Could you describe SPDX-related use cases for your existing OSS risk management routines?
Compatibility	Q2: Could you comment on the compatibility of SPDX specification with your existing OSS risk management routines?
Usefulness	Q2.1: Approximately what percentage of SPDX fields are you currently using or plan to use? Could you comment on the use of these fields or the non-use of others?
Integration Points	Q2.2: Are SPDX fields used for enforcing automatic "gates" in the development build and release cycles? If yes, where would such "gates" be?
Tooling Feasibility	Q2.2.1: Are you using or custom developing SPDX compatible tools to support such "gates"?



<https://github.com/SPDX-CaseStudy/files>



# Answering the Research Question 1

- ▶ RQ1: *How do organizations participating in the SPDX community describe their **local interpretations** of communally structured OSS risk management routines?*
- ▶ **Very differently, ranging from using full standard to learning from early adopters.**
- ▶ *“When I hear my guys having modeling discussions, I often say, ‘look at SPDX, if it's a coin flip what to call this field, let's go with the standard.’”*



## Answering the Research Question 2

- ▶ RQ2: *How do these local interpretations influence the extent of their SPDX **adoption**?*
- ▶ ***Local interpretation is the adoption of SPDX for local needs.***
- ▶ *“The cost of distributing license information was our business driver for adopting SPDX.”*



# Answering the Research Question 3

- ▶ RQ3: *How do these member organizations seek to guide the **advancement** of the shared SPDX specification?*
- ▶ ***Local interpretations are source of innovation for communal practices.***
- ▶ *“[In the SPDX group] we talked about the merits of different fields, how to characterize them, and how to serialize formats.”*



# Discussion

- ▶ **Parallels to other risk related data exchange standards**
  - ▶ Many organizations attempt to address risk close to delivery
  - ▶ Federating risk practices throughout product development can be successful
  
- ▶ **Useful feature of a shared standard like SPDX would be built-in gradation**
  - ▶ Partial and successive implementation enables maturing local practices



# Discussion

- ▶ **Software design is a highly dynamic landscape**
  - ▶ SPDX specification improves guidance by declaring potential risks in OSS
  - ▶ SPDX stabilizes the complexities in software design
  - ▶ SPDX itself entails responsive design within the duality of routines
  
- ▶ **The Open Source Ecosystem has strategic and brokered communities**
  - ▶ Brokers, such as the Linux Foundation, shape the ecosystem
  - ▶ SPDX is one example of a community that enables new interactions
  - ▶ Brokered engagements can include internal communal needs and external needs from brokering foundations



# Contributions to

- ▶ **Routines:** Uncover complexities involved in the development of communal risk related open data standards.
- ▶ **Open source:** Report how the SPDX project is changing the open source ecosystem by developing shared routines and encoding fixed elements in the SPDX specification
- ▶ **Standard setting:** Demonstrate how shared practices shape standards
- ▶ **Methodology:** Demonstrate the use of the assurance case driven case study design.





# Thank you!

- ▶ **Robin Gandhi**  
[rgandhi@unomaha.edu](mailto:rgandhi@unomaha.edu)
- ▶ **Matt Germonprez**  
[mgermonprez@unomaha.edu](mailto:mgermonprez@unomaha.edu)
- ▶ **Georg Link**  
[glink@unomaha.edu](mailto:glink@unomaha.edu)

Assurance case and interview protocol:  
<https://github.com/SPDX-CaseStudy/files>

Full Paper:  
<https://doi.org/10.1145/3148330.3148333>



Robin



Matt



Georg

BRIDGE LAB

UNIVERSITY OF  
Nebraska  
Omaha





18

## Backup Slides



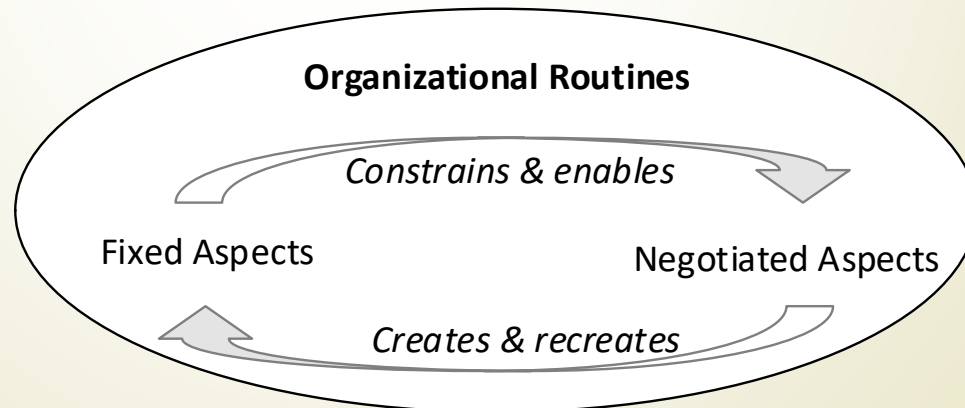
# Key Findings

Rebuttal	Elimination Summary
<b>Rebuttal R1:</b> Unless the SPDX specification is deemed complex for operational needs of local OSS risk management routines.	<b>Rebuttal R1</b> is not eliminated for organizations just starting with SPDX. Organizations engaged in the SPDX community for a long time easily address the rebuttal.
<b>Rebuttal R2:</b> Unless the information recorded in an SPDX document does not support local OSS risk management routines.	<b>Rebuttal R2</b> is eliminated in most organizations by mapping parts of SPDX to local OSS risk management routines.
<b>Rebuttal R3:</b> Unless the organization does not require SPDX documents upon supply or intake.	<b>Rebuttal R3</b> is not eliminated in most organizations as SPDX adoption in OSS supply chains is not widespread. Few organization are starting to use and ship SPDX to customers.
<b>Rebuttal R4:</b> Unless SPDX does not integrate well in to organizational training programs.	<b>Rebuttal R4</b> is partially eliminated by the inclusion of License List in developer training and best practices. However, there is only mention of SPDX in formal training.
<b>Rebuttal R5:</b> Unless engagement with SPDX community is difficult.	<b>Rebuttal R5</b> is eliminated in organizations that directly participate, observe, or engage through proxy representation in the SPDX community. SPDX community is perceived as open and inviting.

Table 1. Rebuttals and summary of findings.

# Exchanging Organizational Routines

- Routine = Set of actions executed repeatedly with reliable outcomes
- Fixed vs. negotiated aspects
  - Fixed: artifacts, workflows, forms, tools, standards, ...
  - Negotiated: actual use, workarounds, shortcuts, ...
- Knowledge boundary complicates exchange of routines



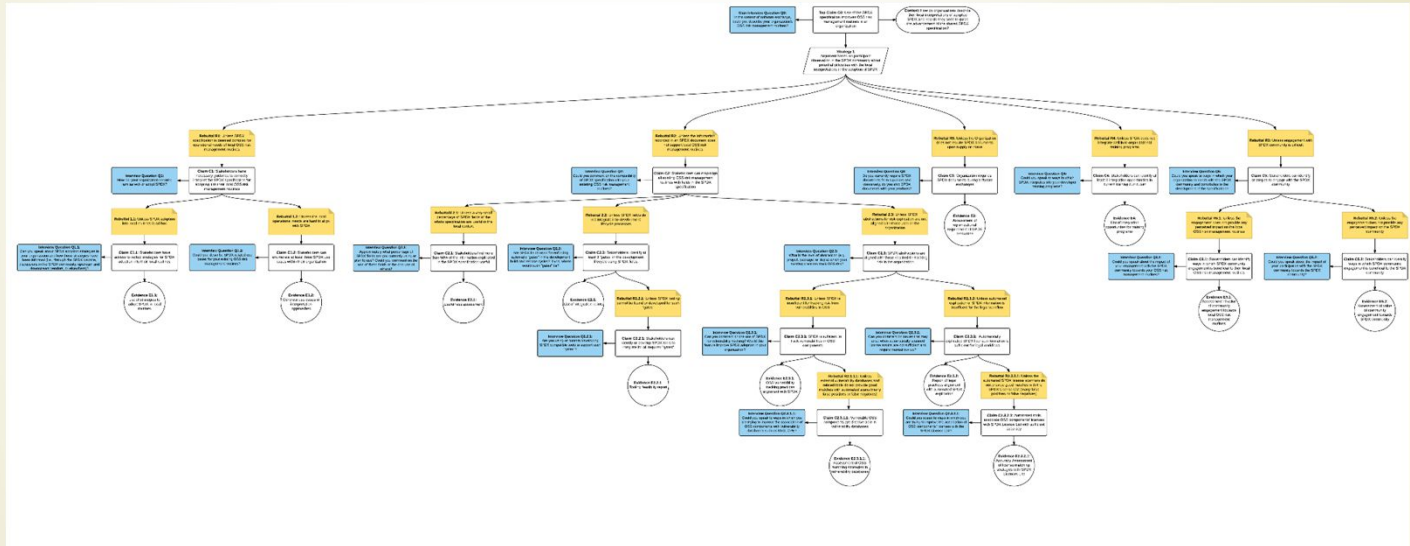


# Creating Shared Routines through Shared Standards

- Shared standards embody the fixed aspects of shared routines
- Achieve compatability and foster exchange
- Requires building shared understanding
  - Adoption is local interpretation
  - Unexpected implementations result from deviant interpretations
  - Audits and certifications assure uniform implementations
- Standardization process benefits participant organizations
  - Align standard with local interpretation
  - Align organization with emerging standard
  - Information advantage



# Method: Assurance Case



<https://github.com/SPDX-CaseStudy/files>



# Assurance Case: Top Claim C0

**Top Claim C0:** Use of the SPDX specification improves OSS risk management routines in an organization



# Assurance Case: Top Claim C0

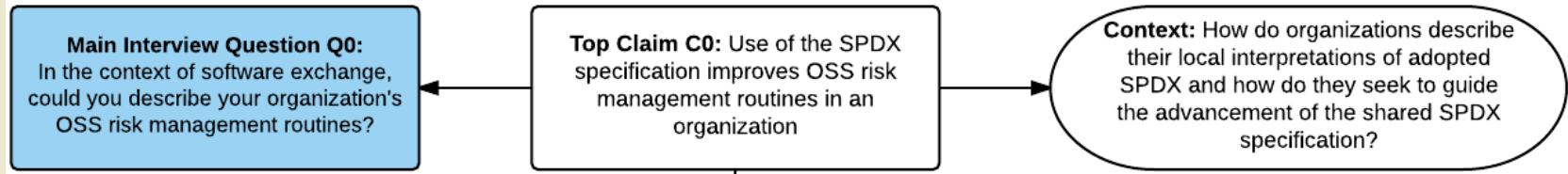
**Top Claim C0:** Use of the SPDX specification improves OSS risk management routines in an organization

**Context:** How do organizations describe their local interpretations of adopted SPDX and how do they seek to guide the advancement of the shared SPDX specification?



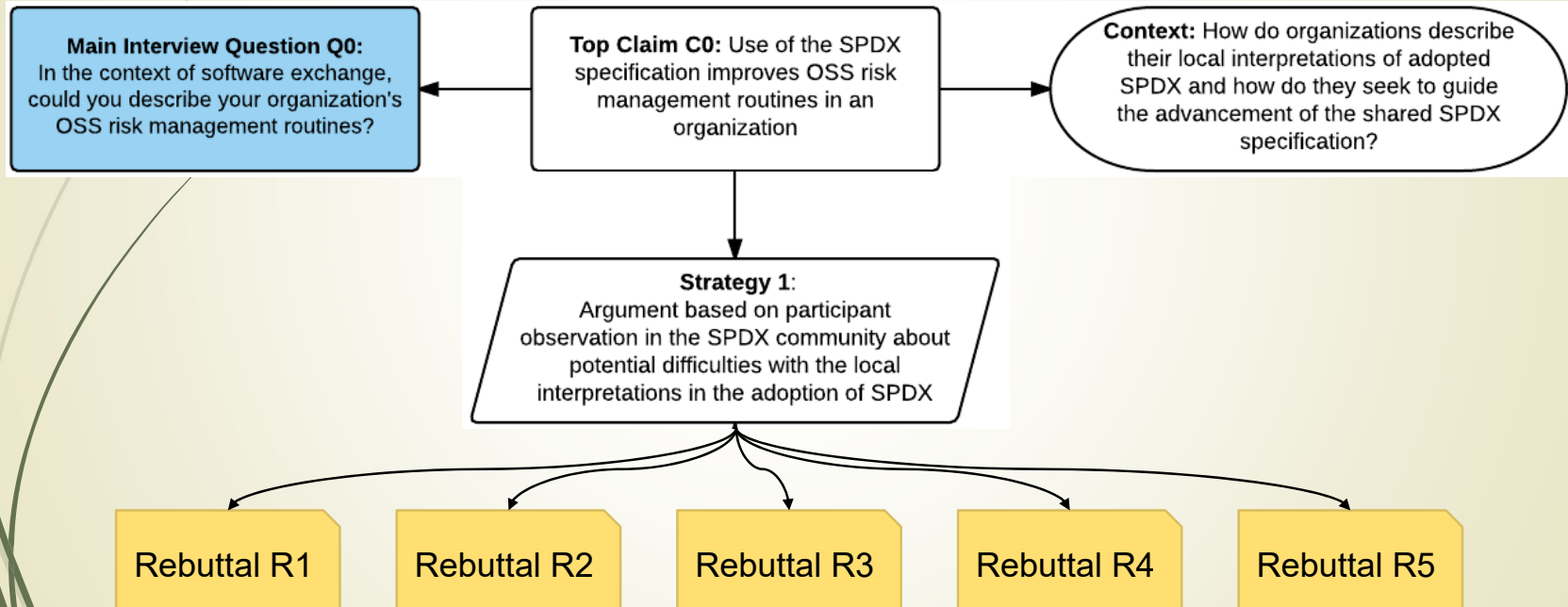


# Assurance Case: Top Claim C0



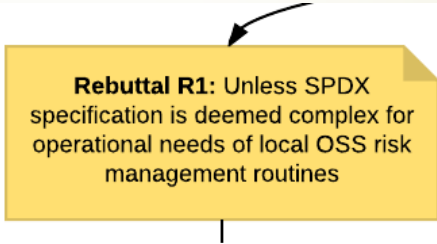


# Assurance Case: Top Claim C0





# Assurance Case: Rebuttal R1



**Rebuttal R1:** Unless SPDX specification is deemed complex for operational needs of local OSS risk management routines



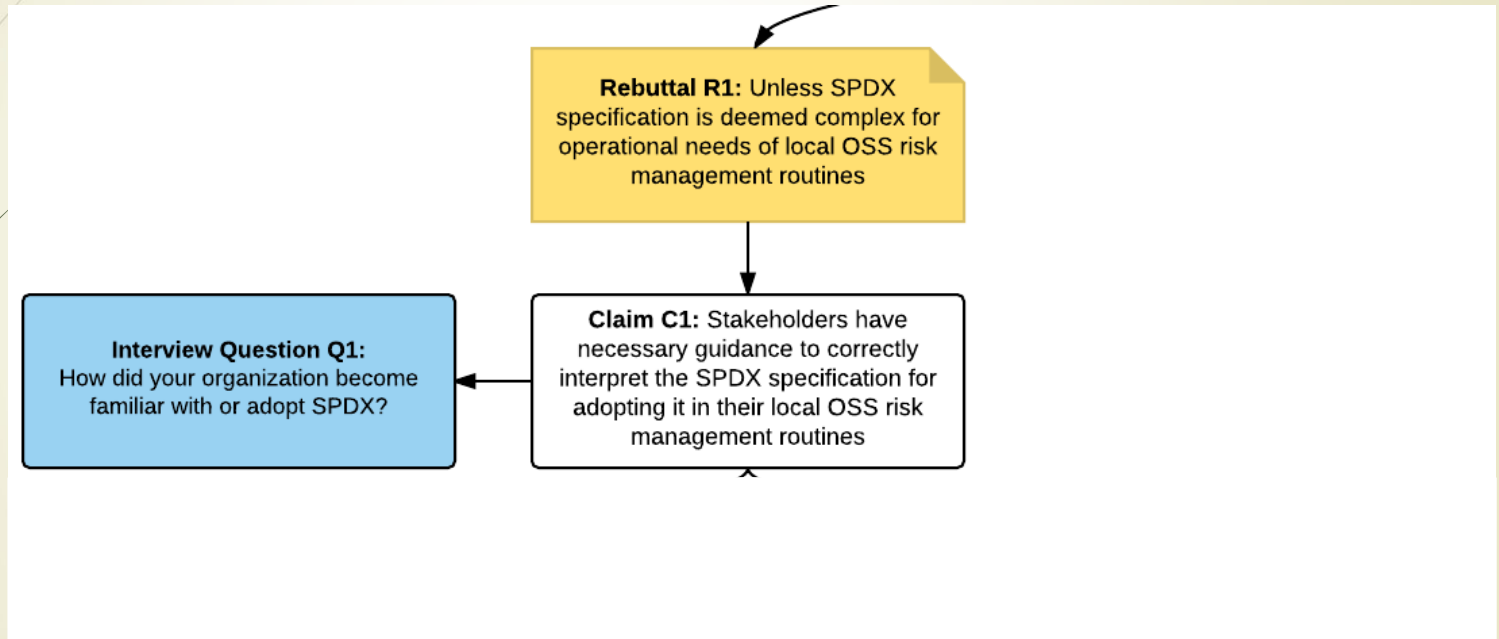
# Assurance Case: Rebuttal R1

**Rebuttal R1:** Unless SPDX specification is deemed complex for operational needs of local OSS risk management routines

**Claim C1:** Stakeholders have necessary guidance to correctly interpret the SPDX specification for adopting it in their local OSS risk management routines



# Assurance Case: Rebuttal R1





# Assurance Case: Rebuttal R1

