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"?
Abstractions	**Q2.3:** What is the level of abstraction (e.g. project, package, or file) at which your existing practices track OSS risk?
External Reference	**Q2.3.1:** Can you comment on the use of SPDX for vulnerability tracking? Would this feature improve SPDX adoption in your organization?
Vulnerability Database	**Q2.3.1.1:** Could you speak to ways in which you are trying to improve the association of OSS components with vulnerability databases such as NVD, CPE?
Scanned Licenses	**Q2.3.2:** Can you comment on issues that may arise when automatically scanned license results are not sufficient and require manual review?
License Matching Accuracy	**Q2.3.2.1:** Could you speak to ways in which you are trying to improve the association of OSS components' licenses with the SPDX License List?
Supply and Intake	**Q3:** Do you currently require SPDX documents from suppliers and conversely, do you ship SPDX documents with your products?
Training	**Q4:** Could you speak to ways in which SPDX integrates into your developer training programs?
Engagement	**Q5:** Could you speak to ways in which your organization connects with the SPDX community and contributes to the development of the specification?
Local Impact	**Q5.1:** Could you speak about the impact of your engagement with the SPDX community towards your OSS risk management routines?
Community Impact	**Q5.2:** Could you speak about the impact of your participation with the SPDX community towards the SPDX community?

Companion to paper: Gandhi, R., Germonprez, M., & Link, G. J.P. (2018). Open data standards for open source software risk management routines: An examination of SPDX. In ACM GROUP '18 Proceedings. https://doi.org/10.1145/3148330.3148333