Notes from 8/28 OpenChain meeting.

== Broad number of attendees, no specific list ==

Shane Coughlan opened by noting the OpenChain Project is making advances in localization. Translations see Japanese getting finalized, and we will soon support Chinese. Our discussion focused on the self-certification web app.

Gary O'Neall noted he backend database and front end ready to be localized using JSON format. This has the advantage that we don't have to wait until upload to know if there are input errors. Localization of different versions of the spec is also being arranged with our prior 1.1 conformance underway. As always our goal is to provide a way for any company of any size to conform for free.

Our assessment of the self-certification web app leads to an interesting observation. Many engaging with the project is not looking for quick conformance. Interestingly many companies are going through our online self-certification to see how close they are to conformance. Our current user interface is an accordion format and companies are using the assessment across the accordion in a non-liner manner. It was discussed that the UI could be made more like the CII best practices, with for example adding a hover-over feature to show the spec language.

The discussion became more general as we moved into adjacent project updates. It was noted there is a stack of open source compliance projects. At the top is the OpenChain Specification, support by online and offline conformance materials. It provides the framework for compliance best practices and these can be (optionally) realized by sister projects like SPDX, FOSSology, Clearly Defined.

We proceeded to have updates from key adjacent projects, starting with SPDX.

Kate Stewart noted that SPDX is made up of identifiers. One of the key things it does is fix errors in the source due to natural language issues. Working with upstream projects, example is ARM MBED, also working with Linux Kernel. Developers are starting to adopt. Then can do a simple Grep on the files, even though there may be other reasons to do scanning. Github API adopted the SPDX standard. Need to move to the file level.

The second part of the project are the SPDX documents. These are upstream to companies and between companies and help to build trust by having the SPDX doc as the BOM. The project has had pockets of success. It has seen adoption for databases internally to companies. There are open discussions about integrating security information into SPDX. XML, Tutu and JSON will be new formats to be supported.

Gary O'Neall noted that we are seeing some other ecosystems like Node and NPM adopt. Some concern over perceived complexity. OpenChain might be able to help to provide context.

Sami Atabani raised a question regarding sharing the scan results; discussion re small number of mandatory fields with many additional optional fields, and extensible. It was noted that this core/ optional format appears to fit in with market requests.

Open source scanning tools like ScanCode, FOSSology can consume an SPDX file, providing a solid foundation for further adoption.

The discussion then turned to ClearlyDefined.

Jeff McAffer provided context that the project allows the sharing of data among companies and allows easier adoption of open source by enterprises. The core approach is to take all the raw results and put them in a store. When you find an error and see that a file needs a license, then can contribute in SPDX format. Community arrives at an agreement. Then will work upstream to trigger a pull request (future feature), then next time it will have the data readily available. How do I know if there is a vulnerability – mapping from a known vulnerability from a candidate CVE. Scanning top files. New files trigger Clearly Defined through an interface, and it pulls the available data. SAP, Google, Amazon, Qualcomm. Standard way to pull out data? Yes, REST APIs for everything. SPDX. When takes FOSSology data, we export the just minimum set we care about. But need to build interfaces to BOM systems.

The discussion turned to OpenChain as a project with a focus on adoption.

It was noted that our format of open meetings is inclusive and welcoming. However, the discussion noted that we may have a challenge in that people do not know which mailing lists to join. It was suggested that we can consolidate to our primary list, but Mark prefers a spec mail list. We noted that having two lists (general and spec) may be preferable moving forward, with the conformance list moved purely to reports of issues regarding self-certification. It was discussed that it may be useful to have an editor role and Shane Coughlan volunteered to look into this.

The discussion turned to OpenChain as a standard, particularly around ISO.

Kate Stewart noted that we should make sure the spec is freely available and asked whether we could use ISO but continue to move as nimbly as we currently can. Shane Coughlan noted that OpenXML gives us the pathway. e.g. ECMA and ISO standard. No need for a pay wall around the primary spec as located in ECMA, while there is the usual minor charge on ISO – content is the same. We think we can manage to stay nimble. Dave Rudin noted there are different ways to bring OpenChain to ISO. Shane Coughlan noted that if we bring the PAS approach for ISO to Gov. Board to take 9mo to 1 year. If we make it general enough, we shouldn’t have to revise it very frequently, which is important for companies like Hitachi – a 5 year iteration is still quite speedy.

Mark Gisi noted that it's a showstopper if it's not open. Sami Atabani noted we should understand what the implications are for OpenChain. Shane Coughlan noted that publishing docs adjacent to the standard means that our hands won't be tied. Sami Atabani noted keeping the conformance process we envision is a key consideration.

Shane Coughlan ended by noting that guided certification as a service via TUVSUD and the like. But we don't want that to undermine the self-certification. Allow the economics of procurement to handle the audit piece. Can get into procurement cycle to accelerate adoption.

The discussion turned to OpenChain as a solution.

Shane opened the discussion to the general question of whether we are providing an adequate solution? Thomas Steenbergen noted that OpenChain takes into account that the world has evolved, but in areas like CI/CD we have few practical solutions in the market, especially in the context of software release to customers multiple times per day. Shane Coughlan noted that we are back to a discussion of levels. Stack, Journey, plus updates from each part of the "Stack". OpenChain can help identify where the stack needs new or expanded projects to address gaps.

Mark Gisi lead the dedicated Spec Team discussion.

The primary discussion was entity level conformance vs. how ISO 9001 does it – consensus in room that we didn't need entity-level provided the recipient knows when they're getting their compliance data from a compliant program.
The secondary decision was regarding training requirement. Balance between being too prescriptive vs. too general. Key outcomes will be shared later.

Nathan lead an Onboarding Team discussion. Key outcomes will be shared later.