

## How TrustSource will help you to align your organisation with ISO 5230

### ISO 5230 (OpenChain) in a nutshell

ISO 5230 was officially adopted by the International Organisation for Standardisation (ISO) on 14th December 2020. This is the first standard for open source compliance, i.e. the legally compliant handling of open source. The contents of the standard originate from the OpenChain project. This is a project of the Linux Foundation, which has set itself the goal of strengthening trust in the use of open source software.

"Open source components from an ISO 5230 (OpenChain) certified organisation are trustworthy".

To this end, the OpenChain project has developed a set of requirements, compliance with which helps to ensure the sustainable use of open source. The specification is currently available in version 2.1. It is public and can be downloaded from the <u>OpenChain</u> website. It defines six goals (Goal=G), which in turn can be divided into eleven essential requirements (Requirement=R). What is special about the specification is that it not only defines the requirements, but also criteria that help to assess the achievement of the requirement. The following figure gives an overview.



This overview is also available as a poster. You can order it <u>here.</u>



In terms of content, five goals ensure the sustainable use of open source software. Four of them focus on the design of the in-house organisation and the fifth on the support of open source projects. The sixth goal concerns the willingness to declare to the outside world that one wants to be measured against the content-related goals, i.e. that one is willing to be certified. The following sections briefly present the goals and requirements and show how TrustSource supports their implementation.

#### G1: Basics / Basis

The first step is to clarify the tasks and obligations within the organisation. This is usually reflected in a policy, an instruction manual for the use of open source software. This describes the roles and their responsibilities, clarifies how to deal with individual cases and describes the processes to be followed.

TrustSource provides a standard policy. It can be used as a starting point for defining your own policy. In addition, the system supports the rollout of the policy (as well as updates thereof) to the area.

shboard	/ Company Polic	ž					ry 카라 tode by entr xish on	New	policy upd	ates	PON	us DULES
	npany po d new policy	olicy					r to execute arbitra	Contribution Policy v1.3 Please review, we described new re View policy file	isponsibilities by role	Upde	n: 15 Mar 2019 ared: 15 Mar 2019 Confirm	
	Active from	Created	Updated 🖕	Policy name	Document	Notify			Presented	Modules over	LICENSES	d
Active				,	2 seament							-

OpenChain further demands that not only a policy exists, but that it is also known to the staff, meaning: "It can be lived". To this end, it must be ensured that the regulations do not only exist on paper but are also known in the software development departments and demonstrably know the contents of the policy.

#### TrustSource provides courses and learning materials that meet the requirements of OpenChain-compliant course training and enable learning checks.

In addition, it is required that procedures exist for the collection and identification of the open source components used as well as the determination of the associated rights, obligations and liabilities.



TrustSource provides a mechanism that surveys the project context and resolves the obligations as well as liabilities from the deployment against this background. Changes to both inventory and objectives are automatically documented.

		✓ Start wizard ② Copy Legal settings from				
Commercial Aspects	Operating Model					
Please indicate commercial purpose intended with the product/service:	How do you plan to operate the solution?					
Yes, a usage fee be charged for the product/service (must be explicitly governed in the contract)	<ul> <li>Solution will be operated in a Software as a Service-Mode</li> </ul>					
Yes, a license fee will be charged for the product (examples include royalties or other types of fees) Yes, but only a support fee will be charged for services provided in addition to the product or service	We plan to operate it on our customer's location(s) as a managed service It will follow a traditional software-distribution model					
Yes, but another type of commercialisation is intended (e.g. maintenance or warranty)	The solution will be part of an appliance / distributed embedded in a device or hardware					
No, the product is not commercial						
Intellectual Property Aspects						
Please specify your intellectual property requirements concerning your own legal safety:						
We do not seek extended protection from 3rd party claims for this module	General Legal Viability CIA History White-/Illackist Custom components Export SPI	0. Danger Operations				
Explicitly reduce risk to be subject to patent claims by the contributors of the open source software			✓ Start wizard ② Copy Legal settings from			
Please specify the power you seek to defend your rights:	Legal requirements		0			
We do not seek enforcement of our claims	This project will commercialize by charging a usage fee					
Retain freedom to enforce own patent claims without risk of license termination Ensure freedom to enforce own patent claims without risk of license termination	Specific needs for the protection of intellectual property were not given as well as an explicit protection of be	ng subject to patent claims from contributors is requested .				
	On the other hand the projects seeks the opportunity to enforce our own claims where necessary .					
Update	Trade Secret Aspects	Licensing Strategy				
	Please specify whether trade secrets (e.g. your source code) in product should be protected:	Please specify the licensing strategy:				
	Yes, trade secrets need to be protected     No, trade secrets may be released	This module shall be licensed under a proprietary license to provide the provided to release the module as open source software				
	Distribution of the module					
	Will the module be distributed?					
	<ul> <li>Yes, it is for use on premise, distributed via separate installer, on physical media or via download</li> <li>Yes, it is as an integral part of an appliance, device or software, which will be shipped</li> </ul>					
urthermore, it is necessary that	<ul> <li>Yes, it is an exchangeable addon to an appliance, device or software, which will be shipped</li> <li>Yes, it is a client side library in a web solution, provided to the user by a webserver</li> </ul>					
-	No, it is a server site library in a web solution, not being distributed					
aterial license obligations are	No, it is applied just locally (e.g., private tool). Module will not be distributed at all					
ocumented for common cases.	opane					

provides a set of rules developed by

lawyers to deal with license obligations, this requirement is automatically met.

### G2: Assigning responsibilities

Since the current documentation situation in the area of open source components leaves a lot to be desired, questions and a need for clarification on the part of downstream users are to be expected. This may concern queries about the use or possibilities of use, but also the components themselves. In order to deal with the enquiries or to receive them in a simple and qualified manner, the specification calls for the definition and communication of a named contact, the "FOSS contact". In addition, there should be a clearly defined procedure for dealing with, processing and following up external enquiries on the subject of "Open source". This is particularly valuable for any later legal proceedings.

With the help of TrustSource, you can delegate this task externally. You set up a mail address and all incoming requests are structured by the TrustSource HelpDesk or processed according to the procedures worked out with you.

In order to meet the requirements, it is considered essential for the process that sufficient legal expertise in the relevant field is available. According to the specification, this may be provided by internal as well as external resources.



The specification also requires that these tasks be provided with sufficient resources. The existence of paper-based processes alone is not enough. The roles must also be staffed with people and it must be ensured that they are given the necessary time to fulfil their tasks.

The higher the level of automation chosen in the context of compliance the fewer resources are actually required. Especially with the highly qualified, often dualeducated IT legal experts, bottleneck is more the norm. With the help of TrustSource, both the analysis and the supervision of projects can be automated to such an extent that single heads can supervise hundreds of IT projects.

### G3: Check and release

The third objective is dedicated to the documentation of the generated software or the artefacts used. The process for generating a bill of materials (BoM) should be sufficiently qualified and documented. Qualified means that the process is suitable for showing the components actually used and ensuring that this information also appears in the BoM.

However, this should not only happen once at a time, but must be done continuously for each release. This is also closely linked to the Medical Device Regulation (MDR). Particularly in the course of continuous deployment, this results in a considerable obligation for the up-to-dateness and archiving of the documentation and the BoMs. Manual implementation, with several builds per day, is no longer conceivable here.

#### Through integration with the development tools, TrustsSource can optimally automate this process. Each version is saved and archived; an up-to-date BoM can be generated at any time.

With the help of a "freeze release" mechanism, certain versions can be specifically held and exposed via API or exported as SPDX.

The specification does not specify the contents of a BoM. However, in the context of the Linux Foundation, the working group <u>SPDX</u> - Software Package Data Exchange - has developed guidelines for the license documentation of an application. These are now available in version 2.2 (3.0 is in progress and candidate for another ISO release). They do not solve the problem conclusively but form a good basis for machine readable BoMs. A newer and lighter alternative is CycloneDX, also a specification for Software Bill of Materials, but somewhat more lightweight.

However, the creation of the BoM alone is not sufficient to ensure safe handling of FOSS. Depending on the use case, the provisions of the now somewhat more than 400 recognised license types<sup>1</sup> can trigger different obligations. For example, the purpose of use, the type of commercialisation or even the form of distribution play a significant role in identifying the obligations to be fulfilled or the obligations triggered.

<sup>&</sup>lt;sup>1</sup> We distinguish here between licence types (MIT, Apache 2.0, etc.) and license variants that result from adapting a license type (e.g. adding a sentence to Apache 2.0), which would not represent a separate licence type.



This is particularly important because some licenses withdraw the right to use the component if the obligations or duties are not fulfilled. In other words, the right to use the component expires if the obligations are not fulfilled. Using components without the right of use in a commercial context is not a trivial offence!

OpenChain therefore calls for a legal review of which liabilities and obligations are to be fulfilled in the respective deployment scenario to ensure a legally compliant application in the respective scenario.

This is where TrustSource comes in. Through knowledge of the conditions and obligations from several hundred licenses and a structured recording of the legal context (use, business model, IP requirements, etc.), the TrustSource rule engine can automatically derive the conditions for use on a case-specific basis and thus make them available as a list of obligations for processing.

### G4: Provide FOSS compliance artefacts

The fourth objective is to ensure that the compliance artefacts are not only generated but also delivered with the generated software. It must therefore be ensured that the artefacts are complete and part of the software.

TrustSource supports this by providing an SPDX document of the corresponding module or project. From v1.8, trustSource also supports the generation of a notice file. A framework for completing the notice file is compiled from the known obligations and the tasks required for completion are identified.

Important in this context is also the use of the *shared-clearing approach*. At the present time, open source components are simply not in a state where one can assume proper documentation. By using a cross-company database for open source components, clearing can be kept

List of obligations	
The following obligations were summarized due to the given legal conditions	
This project will commercialize <b>by charging a usage fee</b> Specific needs for the protection of intellectual property <b>were not given as well as an explicit protection of being</b> <b>patent claims from contributors is requested</b> . On the other hand <b>no specific requirements have been requested to enforce our own claims</b> .	subject to
On the other hand no specific requirements have been requested to enforce our own claims .	
	🕒 Export as PD
Detected obligations	Export as PD
	් Export as PD දා
Detected obligations	
Detected obligations 46 You must provide a copy of the license text.	
Detected obligations 46 You must provide a copy of the license text. This is introduced by:	
Detected obligations         46 You must provide a copy of the license text.         This is introduced by:         th mvn:de.eacg:ecs-gradle-plugin at / 🖸	
Detected obligations 46 You must provide a copy of the license text. This is introduced by:	2
Detected obligations         46       You must provide a copy of the license text.         This is introduced by:            mvn:de.eacgrecs-gradle-plugin at / C	2

to a minimum, as components already revised by others can be reused.



Notice file version 1.0.0 for ECS gradle-plugin					
Export as FDF + Increment version & Freeze version			Completed		
1.2. "Contributor Version" means the combination of the Original Software, prior Modifications used by a Contributor (if any), and th e Modifications made by that particular Contributor.	TODOs Navigator				
1.3. "Covered Software" means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original So ftware with files containing Modifications, in each case including portions thereof.	19 components	21 obligations	5 ToDos remaining		
1.4. "Executable" means the Covered Software in any form other than Source Code.	Academic Free License v1.1				
1.5. "Initial Developer" means the individual or entity that first makes Original Software available under this License.	👩 🔦 License text & Disclaimer				
Disclaimer	🕑 🎰 Data Mapper for Jackson				
UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, MNY OTHER CONTRIBUTOR, OR MAY DISTRIBUTOR OF COVERED SOFTMARE, OR MAY SUPPLIER OF MAY OF SUCH PARTIES, BE LIABLE TO MAY PE	Apache License 2.0				
RSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOOWYLLL, NORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SH ALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABLITY SNALL NOT APPLY TO LIABLITY FOR DEATH OR PER	Common Development and Distribution License 1.0				
SONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTAL DAVAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.	🗌 🔦 License text & Disclaimer				
ALLOW THE EACLOSION OF LIMITATION OF INCLUENTAL OF CONSEQUENTIAL DWHACES, SO THIS EACLOSION AND LIMITATION PAT NOT APPET TO TOU.	<ul> <li>H- JavaBeans(TM) Activation F</li> <li>ModifiedSources</li> </ul>	ramework			
This license applies to the following components:	Modifications				
JavaBeans(TM) Activation Framework [1.1.1]	Common Development and D	istribution License 1	1		
The JavaBeans(TM) Activation Framework is used by the JavaMail(TM) API to manage MIME data		Secon Electibe 1.			
This component has been modified. 🧨 Changes url: has not been provided Changed sources url: has not been provided	Creative Commons Zero v1.0	Universal			
	MIT License				

In order to act in a legally compliant manner, it is also necessary to establish revision security. This means that old versions must be kept at least until it is certain that no old version is still in circulation. This is necessary so that questions about an older version can be answered on the basis of a secure document.

## TrustSource can provide the information on all versions created in TrustSource again at any time.

On this basis, it is always possible to identify which components were used where or when and under which conditions. On the one hand, documentation makes people vulnerable, as it also documents what has not been done. On the other hand, it also leads to the certainty of having actually done everything necessary to establish legal certainty. With such an approach, it should be possible to detect errors in good time.

#### G5: Understanding community commitments

Open source is not a one-way street. One should not only take, all users of open source are also invited to contribute. This happens through collaboration in the open source projects, so-called *contributions*.

To this end, in-house resources are usually seconded to the open source project for a period of commitment, either to work on the project in full or in part. Depending on the intensity, this can be done on an occasional basis in the form of bug fixes or voluntary additions, or as a defined secondment to the core of the project. Depending on the intensity, it opens up influence on the design of the product to the contributing company. It is also conceivable that the company creates its own open source project.



Whether occasional or targeted and structured, whatever form is chosen, contributions must be clearly regulated. This involves legal issues such as the separation of working time and free time, claims and rights arising from contributions to open source projects, as well as the process for making contributions available.

The fifth goal addresses the issue of playing back into the open source community and requires that there be a policy regulating the handling of or contributions to open source projects. Analogous to the regulation for the use of open source in the company, it must also be ensured that the regulations are sufficiently disseminated and known.

The regulation for participation in open source initiatives can also be used with the help of the same mechanisms as the support to G1. TrustSource also offers a sample policy as a basis for the design of contributions.

It may be that the regulation prohibits participation in open source projects. In this case, only the publicity of the ban should be propagated. From our experience, however, a ban does not lend itself to this. As soon as open source is used seriously, bugs in the software used are to be expected. It would be negligent not to be able to fix them because of a ban on contributions.

Accordingly, a governance process must be defined for the contributions. Ideally, this should not differ significantly from the process for own products in order to make it easy to handle for all parties involved.

TrustSource provides a uniform platform for both forms of use with comprehensive tools for process support.

### G6: Effort to certify conformity

The sixth goal requires the organisation's willingness to confirm the implementation of the requirements from goals 1-5. This is currently possible with the help of a self-audit. The OpenChain website offers a questionnaire for this and corresponding OpenChain partners support the implementation.

# TrustSource provides a suitable platform to ensure the processes. This is known by the certifying parties and simplifies the clarification of the audits.

### Summary

In summary, it can be seen that the company-wide use of TrustSource can significantly reduce much of the complexity of an OpenChain-compliant alignment of even a larger organisation. However, it also remains to be noted that OpenChain requires the introduction of processes and the change of procedures. This is always an elaborate undertaking that requires time and focus.



We therefore recommend choosing the scope specifically. It may well make sense not to start with the introduction at group level, but to concentrate on a single entity first. With the experience and success stories, the introduction in a second area can be achieved much faster.

TrustSource can also help here in the enterprise version with the multi-entity option. This makes it possible to combine individual units/areas in one account and administer them across the board, but to provide them with area-specific policies or blacklists and whitelists.

TrustSource can also help unify results for organisations that already use other scanning tools in some areas. With the ability to submit scan results to the TrustSource API or import SPDX documents, TrustSource can serve as the link across multiple, possibly already existing, areaspecific tools. In this way, process conformity and uniform governance can be ensured throughout the company.

TrustSource also supports other aspects of software development. For example, test reports and other information can be archived and thus tied to specific releases. Vulnerability analysis is supported and technology management is automated. By using black, white and grey lists, components classified as obsolete can be identified before they are used and their use can be prevented. for more information, see <u>https://www.trustsource.io.</u>

If you have any further questions about TrustSource or OpenChain, please do not hesitate to contact our colleagues. You can reach us at <u>sales@trustsource.io</u> or <u>sales@eacg.de.</u>