ORCRO

AN INTRODUCTION TO OPENCHAIN

ISO/IEC 5230:2020

A SCALABLE, COST-EFFECTIVE ROUTE TO MINIMISING RISK IN THE SOFTWARE SUPPLY CHAIN, RECOGNISED BY INDUSTRY AND BACKED BY THE LINUX FOUNDATION.

OPENCHAIN

“The services provided by Andrew Katz and his team at Moorcrofts and Orcro were outstanding. They not only provided the technical legal advice for us to be able to reach the OpenChain conformance standard, ensuring our component database contained the relevant open source licences, they also worked with our team to establish an appropriate open source policy, tailored to B2M’s specific business needs, and provided the compliance training to our developers.”

Julie Purves, B2M Solutions CEO

EXECUTIVE SUMMARY

ISO5230:2020 (OpenChain) brings established governance principles to the software supply chain. It adopts best-practice compliance principles from other compliance areas, such as data security and privacy, and creates and maps them on to software procurement, giving businesses a clear path to minimising risk in procuring, developing and deploying software, with particular emphasis on use and re-use of free and open source software ("FOSS") components.

Crucially for smaller organisations the programme does not have to be complex but simply mirror or adapt existing best practice.

The OpenChain project is backed by the Linux Foundation, and is the only compliance project designed with the following factors in mind:

- Adopts structure of other standards (such as ISO 27001)
- Released by ISO as an international standard in Q4 2020 (ISO 5230:2020)
- Flexible and versatile: scales with size and type of business
- Backed by industry participants of all sizes
- Developed with input from software engineers, legal, compliance, management and procurement.

OpenChain manages the legal and associated reputational risks of software licence non-compliance, providing comfort to your customers, and easing engagement with your own suppliers.

Self-certification provides an inexpensive and rapid path to compliance, but for additional security, Orcro Limited, in partnership with its sister company Moorcrofts LLP (one of the first five worldwide pathfinder partners appointed by the Linux Foundation), can guide organisations through the process, culminating in an external certification of compliance, as a step beyond self-certification.

OpenChain has been adopted by companies as diverse as:
Google
Facebook
Uber
Adobe
Cisco
Arm
Synology
Hewlett Packard Enterprise
Sony
Qualcomm
Toyota
Siemens
New organisations, large and small, are joining every day.

REDUCE RISK

MINIMIZE IP RISK

ROBUST PRACTICES

QUICKER AND SAFER

WHY DO WE NEED OPENCHAIN?

OpenChain has two main functions: it provides a framework to reduce risk for a company's internal software development processes, and it reduces friction and risk in the supply chain by making it quicker and safer to procure software and components incorporating software from third party suppliers.

From an internal development perspective, OpenChain ensures that a company knows and understands how to deal with open source code, and has robust practices and procedures around selecting, incorporating, using and deploying open source code in compliance with its licences.

When a company is procuring software from third party suppliers, if those suppliers are OpenChain conformant, the purchaser can take comfort that the product they are purchasing has been built using a programme designed to minimize IP risk, and will be supplied with the relevant compliance materials. OpenChain benefits both developers, and procurers of code.

As businesses become less vertically integrated and rely on an increasing web of suppliers and sub-contractors, supply chains become more complex. More complex supply chains mean increased opportunities for poor components to lower the overall quality of the end-product, and ultimately, to potentially cause an end-product to fail, causing loss and damage. A quality procurement process minimises the risk of this failure by:

- Facilitating due diligence at the outset of a supplier relationship;
- Providing transparent and consistent documentation to make an informed choice between competing suppliers;
- Assisting management of the relationship once it has formed;
- Easing the negotiation and management of supply contracts;
- Providing a framework for monitoring and assessing quality over time;
- Providing traceability of problematic components; and
- Providing a transparent and effective mechanism for handling issues that may arise.

In areas as diverse and food and pharmaceuticals, these supply chain management practices and standards already exist. Software procurement, and especially software procurement involving free and open source software, has, until now, lacked this maturity.

OpenChain is increasingly being used as a framework to assist in the due diligence process for mergers, acquisitions and fundraising. An OpenChain conformant business will be quicker and easier to fund, float or sell.

OpenChain takes existing, proven, supply chain practice and procedure and maps them onto software procurement.

WHAT ARE THE RISKS OF NON-COMPLIANCE?

Software development increasingly consists of the integration of components from different sources. Many are likely to be open source components, such as Drupal, Apache, MySQL or Neo4j, and they may be combined with proprietary components and libraries from companies such as Microsoft or Oracle. We have clients with software consisting of over 100,000 separate components, from different projects, under different licences. The final product may be deployed on-premise, embedded in a device (which itself can range from a mobile phone to a motor vehicle) or supplied on a SaaS basis. In each case, the product must be licensed to end users in a way which is compliant with every single one of the licences under which the components are provided. In addition, the end user must also be provided with documentation such as copyright notices and copies of the licence text, where required by the licences of the components. Source code may also need to be provided for some or all of the code.

Any one of those components may present a risk (for example, it may contain unlicensed code), and a combination of components may be incompatible with the intended method of supply to the end user (for example, software which is fine to provide on a SaaS basis is not necessarily licensed for use on-premise).

In each case, the software deployed may be business critical. The loss of use of that software (potentially through non-compliance affecting only a single component) can cause catastrophic business loss, and ultimately failure.

Potential points of failure include:

LEGAL RISKS
Injunction granted for licence violation, damages, exposing customers to potential claims and, in extreme cases, the requirement to release and license the source code of the business's core code;

TECHNICAL RISKS
Failure of software to perform to specification, bugs;

SECURITY RISKS
Vulnerability to data breaches or sabotage.

OpenChain's primary focus is on legal risk, but by promoting active best-practice in project selection and traceability, and encouraging engagement with FOSS projects, it has the secondary benefit of reducing risks across the software development and procurement activity.

HOW DOES OPENCHAIN ADDRESS THE RISKS?

Risk can be addressed in three ways, by managing it through process and procedure, by passing it to another party (through insurance, for example), or by negotiating contracts which minimise exposure. Of these three methods, only process and procedure eliminate risk at source.

OpenChain helps an organisation to select, develop and deploy software in accordance with a set of policies and procedures which are designed to minimise risk by ensuring that the software is selected from reputable and verifiable sources, has appropriate licences attached to it, that the components are all traceable and have the necessary information attached to them, and that they are made available to end users in a way which is compliant with the licences attached to them.

The policies and procedures are not imposed on the organisation: they can (and should be) developed with the organisation's culture and business aims in mind, so long as they adhere to the fundamental principles of OpenChain.

Irrespective of the detail of its practices and procedures, an OpenChain conformant organisation must demonstrate that it:

- Knows and understands its responsibilities in software licensing, including FOSS, and has an appropriate policy for selecting and deploying software;
- Has identified the roles played by individuals in exercising, managing and reviewing the OpenChain programme, and ensures that the roles are appropriately staffed, empowered and resourced;
- Gives relevant staff appropriate training;
- Has a process for reviewing software licences;
- Has individuals appointed in relevant liaison and compliance roles;
- Obtains and archives appropriate provenance and licensing information for all software components it deploys;
- Has a process for dealing with exceptions to the selection policy;
- Provides the customer with all materials required by the relevant licences;
- Has, and follows, a management programme which implements the above requirements.

WHAT DO YOU NEED TO DO?

Nothing in OpenChain requires that conformant organisations must engage a third party organisation to certify compliance. Self-certification is a potential route to compliance. However, this process can be time consuming, and there is no guarantee that self-certification will give your customers the peace of mind they require. The information you need to ensure compliance, and self-certify, can be found at openchainproject.org.

ALTERNATIVELY, YOU CAN ENGAGE ORCRO TO GUIDE YOU.

Orcro is accredited to provide ISO certifications by the OpenChain Project, Linux Foundation to companies who have achieved and is maintaining the OpenChain governance principles which meets the requirements of the standard.

WHAT IS THE PROCESS?

Even though OpenChain itself is new, the route to compliance is similar to the process we have been implementing for our clients for some time, but now with the added benefit of an industry-recognised outcome, and a certification you can promote to your customers.

Orcro can guide you through the process, assist you to develop practices and procedures which are both OpenChain compliant, and, crucially, are tailored to your existing practices, culture, and business aims, and, finally, providing a letter of conformance.

We operate on a staged basis, and aim to give costings for each stage as part of the deliverables for the previous stage. We operate on an agile basis, and, unless you have authorised us to incur third party expenses or bring in external partners, you can terminate your engagement at any time, and are only committed to paying for work done until the point of termination.

WHAT DOES OPENCHAIN VERIFICATION AND CERTIFICATION MEAN?

If you receive certification and verification from Orcro, it means that

1

Your processes and procedures covering software licence compliance risks are verified as robust, reducing your risk of non-compliance.

2

You can reassure customers that you have met the certification, it has been verified by a trusted third party, and that you have verifiable and solid set of practices and procedures.

3

You are able to simplify contract negotiations with your customers, by being able to warrant that you are OpenChain compliant.

4

You will have a 'compliance pack' to hand, which is essentially a compliance dossier. This is an invaluable resource you can provide (under NDA where necessary) to customers, prospective customers, investors, insurers and funders to demonstrate compliance and maturity.

5

You are able to supply to the increasing number of large organisations requiring OpenChain compliance as a precondition of becoming an accredited supplier.

THE OPENCHAIN ROADMAP

OpenChain adoption is rapidly growing, and as adoption continues, members are more likely to request, and subsequently demand, compliance with OpenChain as a precondition to appointing software suppliers.

The OpenChain project has released the OpenChain Security Assurance Specification 1.1. Building on the OpenChain specification for open source licence compliance, the assurance specification provides a framework for ensuring that an organisation has in place robust procedures for identifying and remediating publicly known security vulnerabilities in your code. The Security Assurance Specification will be submitted to the ISO/IEC standards process.

THE ORCRO COMPLIANCE PROCESS IN DETAIL

STAGE 1

PROJECT SCOPE AND UNDERSTANDING

During this stage, we work with you to determine your business aims, culture and management structure, as well as acquiring the data necessary to begin the path to compliance. Because compliance can be achieved in a number of ways, the precise route will depend upon the information gathered in stage 1. We regard culture as particularly important, as issues such as appetite for risk, attitude towards openness, whether software freedom is more important than maximising the use of developed software, willingness to become involved with (or establish) free and open source project communities, and how those qualities are communicated to and valued in staff, are vital to ensure that the route to compliance and certification is deeply compatible with your aims.

STAGE 2

KNOWLEDGE ACQUISITION

The second stage involves acquiring more detailed information, and is likely to require input from your subject-matter experts. In particular, this will likely involve an overview of possible analysis of actual coding working practices, review of structure of repos and any code-scanning database, and review of specific documentation such as assignments, licences and EULAs.

It will be at this stage that the scope and aims are more clearly defined. However, it may also be the case that specific client-facing issues are relevant, such as requests for certain forms or warranty and indemnity over provenance and IPR liability, and the scope of the engagement may be adjusted to deal with this (for example review of appropriate liability clauses within EULAs etc. to refer specifically to certification, or to permit the release of certain compliance materials under NDA). We will typically require access to your repositories for this, and one option is to set up a data room where relevant compliance materials such as policies and procedures can be uploaded.

STAGE 3

REPORT ON CURRENT STATUS

The third stage involves producing a comprehensive report setting out the current compliance status, with detailed recommendations as to next steps. After consideration and discussion of the content of the report, we will agree a compliance programme with you based on the recommendations set out in the report. We will also make recommendations as to whether the work should be carried out by the Orcro compliance team, or whether it should be carried out in-house.

STAGE 4

IMPLEMENTATION STAGE

Stage 4 involves implementation of the recommendations, either by your internal team, or with the involvement of Orcro in each case as agreed with you. This may include drafting of appropriate policies and procedures, assisting with practical aspects of implementation, providing training (on either a direct-training or train-the-trainer basis) and assisting in establishing and documenting procedures, as well as additional work agreed within the scope for Stage 2. It may also involve updating existing documentation (such as client terms and conditions and SaaS service agreements, third party supply agreements, such as hosting agreements, development agreements, subcontractor agreements and testing and quality control services agreements).

At this stage, you may opt to self-certify that you have the relevant practices and procedures in place, although we are unable to provide a letter of confirmation until after the audit and review stage.

STAGE 5

AUDIT AND REVIEW STAGE

Stage 5 involves an audit of the processes and procedures as implemented in Stage 4 against the Open Chain Specification. Where there are non-compliances, Orcro will work with you to address them. This may also involve input from third party experts (for example, to check that firmware loaded into shipped devices corresponds with the source made available).

The key deliverable is a letter of advice, which may be made available to your customers, certifying that our client has achieved compliance with the current OpenChain Specification.

(Important: nothing requires our client to obtain such a letter of advice before describing itself as compliant: it is open to our client to assess its own level of compliance against the OpenChain criteria at any time, and if it is satisfied it has met the criteria, to describe itself as having achieved self-certified compliance.)

STAGE 6

INDEPENDENT AUDIT

We are able to offer a third party independent audit service. Where we have advised on OpenChain compliance and implementation, you will work with a separate Orcro audit team which has not been involved with the consultancy team, and works to a robust ethical wall procedure, approved by the Linux Foundation. This means that we are able to provide and end-to-end service, enabling you to achieve an OpenChain certification which has been approved by the Linux Foundation. We are authorised by the Linux Foundation to provide both Systems Certification and Program Certification, to provide independently verified confirmation of software development to the ISO 5230:2020 standard. Two Levels of audit are provided. Programme certification, which confirms that a compliance programme, when operated correctly, fulfills the OpenChain requirements. The second (Systems Certification) looks back over the actual operation of the programme and certifies that operation of the programme has been succeeded.

STAGE 7

ONGOING SUPPORT

We will (if requested) make ourselves available to address licensing queries as they arise from time to time, and also to regularly test compliance with the Specification, and renew the advice letter (if requested) from time to time, in the light of updates to the OpenChain Specification or the adoption of additional modules. We are also able to renew OpenChain Certification.

WHY ORCRO

Orcro Limited is established to undertake compliance services, and is a sister company of the long-established UK technology and corporate law firm Moorcrofts LLP. Moorcrofts has been at the forefront of Free and Open Source Software licence compliance in the UK for many years.

We have established compliance programmes for many organisations ranging from startups to multinationals, and regularly work with some of the most respected companies and individuals in the field worldwide.

In fact, our involvement with OpenChain at a very early stage means we have been able to influence the direction of development of OpenChain as a whole, and as one of the first five partners appointed by the Linux Foundation worldwide, we are very well placed to give or clients an early steer as the roadmap for development.

We are currently working with the Linux Foundation on expanding the guidance and materials for OpenChain which are being made publicly available. Andrew Katz chairs the OpenChain UK Work Group (see openchain.uk).

Version 2.1 of the OpenChain specification has been accepted as a formal international standard by the International Standards Organisation, under ISO 5230:2020. The OpenChain Security Assurance specification is in the process of becoming an international standard.

Orcro was the second organisation in the world, and the first in the UK, to provide official certification services for the new ISO OpenChain standard.

We have regularly presented at and participated in conferences and initiatives involving Free and Open Source Software worldwide, making us a thought leader in the field.

We combine unique compliance engineering and legal expertise to provide a one-stop-shop to open source software compliance.

MEET THE TEAM

ANDREW KATZ
CEO

TIM ASTLEY
HEAD OF AUDIT

ALEX MURPHY
COMPLIANCE ENGINEER

USHA GUNESS
SENIOR CONSULTANT

FINNIAN ROBINSON
LEGAL AND COMPLIANCE
COORDINATOR

Andrew, Tim and Usha are qualified solicitors at sister firm Moorcrofts LLP, all specialising in technology law.

> “I have worked with Andrew on matters related to open source, compliance and broader governance for more than a decade. The breadth of his knowledge is considerable, not least due to his extensive understanding and experience of technical matters. Moorcrofts is my “go to” recommendation for anyone doing business in the UK and Andrew is one of the experts I keep on my speed dial. You simply cannot do better than working with him.”
>
> *Shane Coughlan, General Manager, OpenChain Project.*

ORCRO

+44 (0) 203 7930343

team@orcro.co.uk

orcro.co.uk

83-85 Baker Street

Marylebone

London

W1U 6AG

Thames House

Dedmere Road

Marlow

Buckinghamshire

SL7 1PB

OPENCHAIN

Orcro Limited is registered in England & Wales under Company Number 11173406.
Registered office at the Marlow address above.