

# Introducing OpenChain

A tested framework for open source compliance.

Andrew Katz

[www.moorcrofts.com](http://www.moorcrofts.com)

# Finance Sector

## Risk Management

# Finance Sector

## MIFID II

# Finance Sector

## MIFID II - Outsourcing

# Finance Sector

## MIFID II - Outsourcing

# MIFID II

## Outsourcing

“...avoid undue additional operational risk”

Art 16(5)

# Managing Risk

- Passing to provider (contractually)
- Passing the risk to a third party (insurance)
- Identifying, minimising and managing risk

# Managing Risk

- Passing to provider (contractually)
- Passing the risk to a third party (insurance)
- **Identifying, minimising and managing risk (process)**



# Software-related risks

- **Functionality**
- Security
- Licensing/IP

# Software-related risks

- Functionality
- Security
- Licensing/IP

# Software-related risks

- Functionality
- Security
- Licensing/IP

# Functionality

- Trusted source
- Quality assurance

# Security

- Trusted source
- Quality assurance
- Pen-testing / fuzzing
- Linux Foundation Core Infrastructure Initiative
- SAFECODE
- Tooling (BlackDuck, Flexera)

# Licensing/IP

- Trusted source
- Licence compatibility
- Tooling (BlackDuck, Flexera, Quartermaster...)

# What if it all goes wrong?

Damages

Injunction

Outsourced provision ceases



# Damages Injunction

Outsourced provision ceases

Damages  
Injunction  
Outsourced provision ceases

# CONTEXT





# Modern Software Development



# Assembling components

# Code Club (Sandwich)



..... Choose a Framework

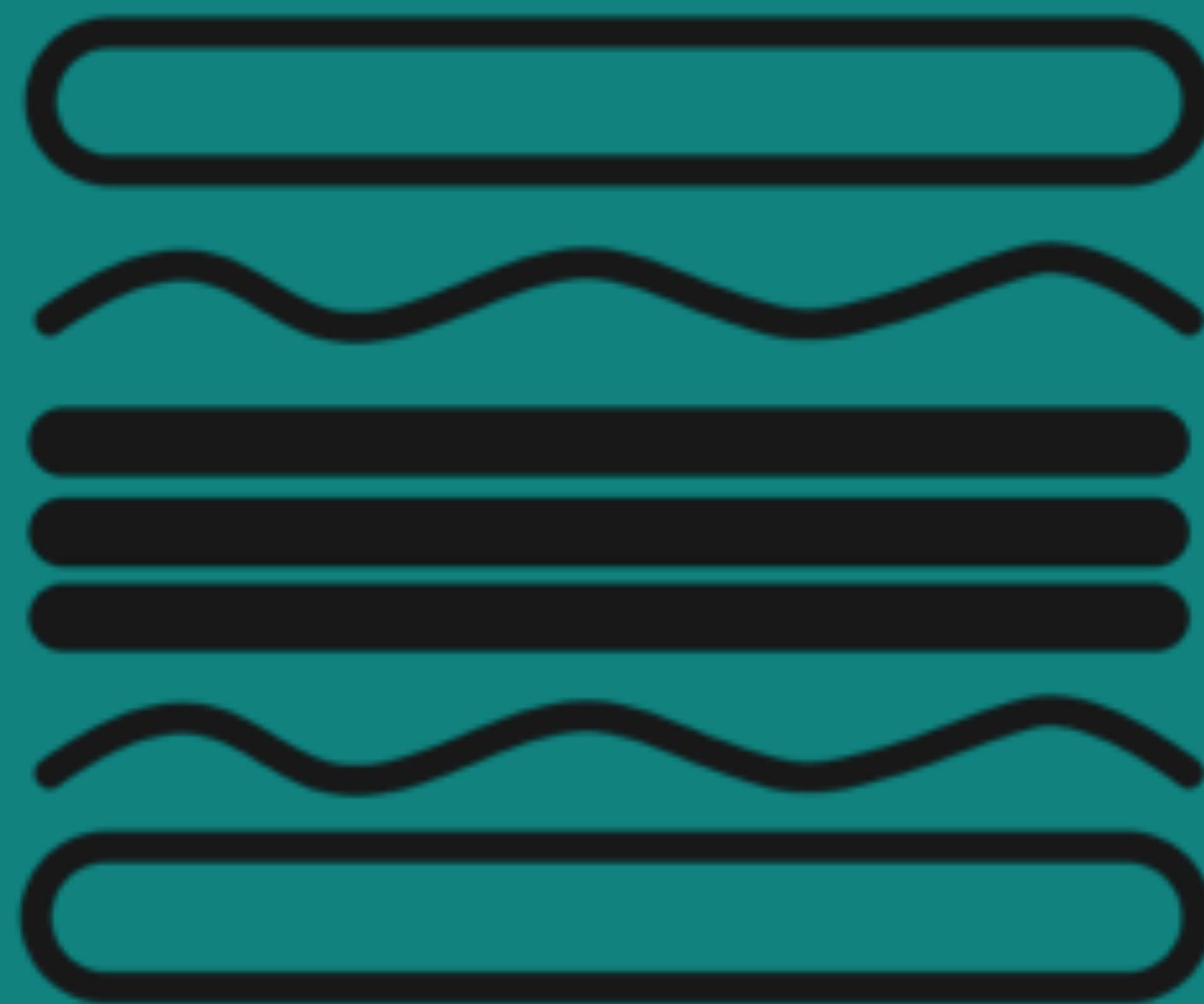
# Code Club (Sandwich)



Write Custom Code

Choose a Framework

# Code Club (Sandwich)



Use Open Source

Libraries to Solve Problems

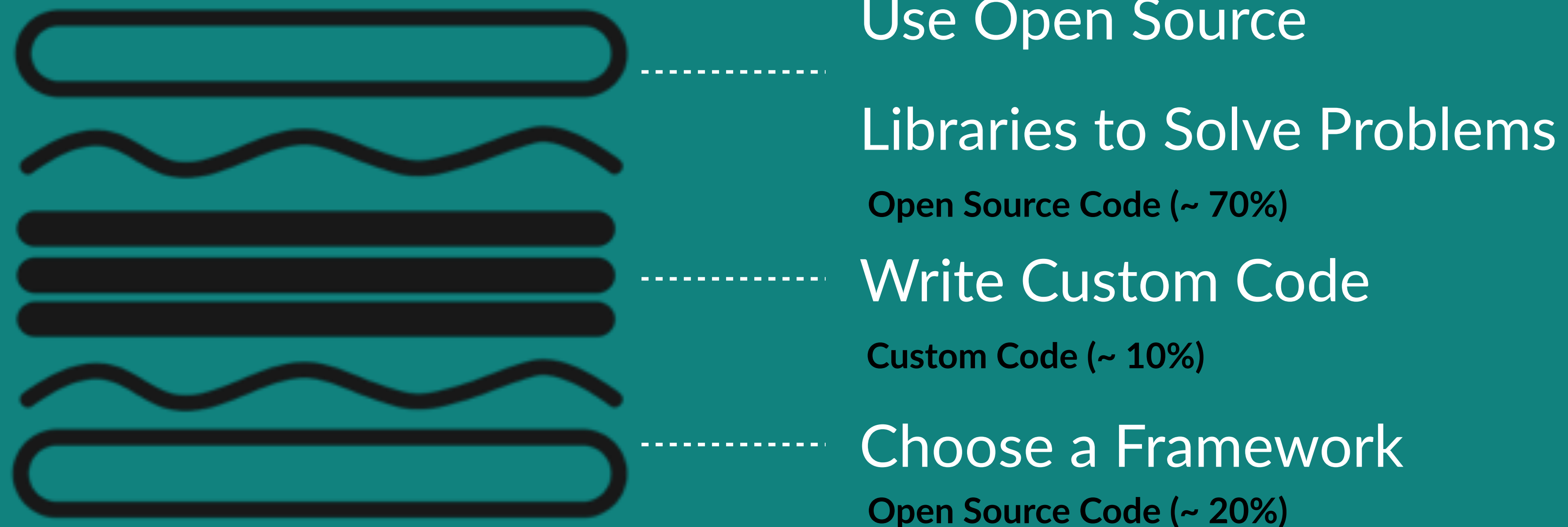
Write Custom Code

Choose a Framework



# Code Club (Sandwich)

Open Source Code = ~ 90%



Many different sources:

- Sourceforge
- GitHub
- Maven Central Repository

Every component is  
subject to copyright\*

Every copyright work  
can only be used if  
correctly licensed\*

=> every component  
must be properly  
licensed

# What happens if components are not correctly licensed?

# Linksys WRT54G





## Scenarios:

- Infringement claim
- Due diligence on IPO/funding acquisition
- Customer due diligence - e.g. MIFID
- Whole codebase inadvertently open sourced
- Forced release of source code\*

# How do you demonstrate compliance?

# Code analysis

# Licence analysis

# A truism about due diligence:

A truism about due diligence: it's not so much about the information, as the process.

# Characteristics of an open source compliance programme:

1. Verify that the company is compliance with licences

2. Put in place good practices and procedures

- open source policy
- training for relevant staff
- licence review policy
- responsibilities are identified, roles empowered and funded
- bill of materials for products are generated
- open source programme handles common licence issues
- appropriate compliance materials are provided with the software
- there is a contribution policy for external projects



COOPENCHAIN

 **OPENCHAIN**

 **THE LINUX** FOUNDATION **PROJECTS**

 **OPENCHAIN**

**TOYOTA**

  
**CISCO**

**arm**



**Hewlett Packard  
Enterprise**

**HITACHI**  
Inspire the Next

**QUALCOMM®**



AN INTEL COMPANY

**SIEMENS**

# What is OpenChain?

# The OpenChain project addresses the question...

# How do I trust FOSS compliance in the supply chain?

It's:  
*a standard* to describe  
what organisations could  
and should do to address  
FOSS compliance  
efficiently;

It:  
identifies key  
recommended *processes*  
and *record keeping*  
requirements for effective  
FOSS management;



It:  
builds *trust* and *increases*  
*efficiency*, by having FOSS  
processes and record  
keeping *consistent* across  
the supply chain

It consists of 3  
components:

1.

2.

3.

It consists of 3  
components:

1. Specification

2.

3.

It consists of 3  
components:

1. Specification
2. Curriculum
- 3.

It consists of 3  
components:

1. Specification
2. Curriculum
3. Conformance

# Specification

# Specification

*...defines a core set of requirements that every compliance program must satisfy.*

# Curriculum



# Curriculum

*...provides the  
educational foundation  
for FOSS solutions and  
processes*

# Conformance

# Conformance

*...the way an organisation  
can demonstrate its  
conformance with the  
specification*

# Find out more at:

[\*openchainproject.org/spec\*](https://openchainproject.org/spec)

[\*openchainproject.org/curriculum\*](https://openchainproject.org/curriculum)

[\*openchainproject.org/conformance\*](https://openchainproject.org/conformance)

The aim:

*to build trust, by creating a  
web of organisations which  
are conformant with the  
OpenChain specification*

*“There is nothing in the OpenChain specification which well-run FOSS-developing companies are not likely to be doing already.”*

# What does conformance require?

You need a FOSS  
policy, and you need  
to show that relevant  
staff know about it  
and have access to it.



Relevant staff need training in

- your FOSS policy,
- basic licensing law, concepts and principles,
- internal roles and responsibilities

You must have a process to...

- establish the appropriate licence for each component used
- determine the restrictions and obligations applicable to each licence

You must have appointed someone with responsibility for

- FOSS liaison (external)
- FOSS compliance (internal)

...and the roles must be sufficiently senior, and properly resourced.

You must have a process to...

- create and establish a bill of materials for relevant software; and
- ensure that the licences etc. for each item are correctly assigned

**Your licence management processes must identify and deal appropriately with common FOSS use cases (e.g. copyleft, modified code, licence incompatibility)**

You must have prepared the appropriate materials accompanying a distribution of the software to ensure compliance with the licences, such as source code, offer notices, attributions, NOTICE.TXT, licence text

You must have a policy covering contributions by the organisation to FOSS projects.

You must certify that  
you comply with the  
specification's  
requirements.



You can self-certify, but as the OpenChain project evolves, we expect organisations to seek external, independent verification.

## Roadmap....

- members will encourage/prefer/require compliance from suppliers
- eases supplier due diligence
- standardises availability of compliance documents
- warranty of compliance
- virtuous circle

# CASE STUDIES

Software company selling cloud services to pension providers  
Their regulated clients require DD on the code as part of their own risk management.

They are now able to provide those clients with the materials required by OpenChain certification

20 developers, c100 different packages.

Software company providing sector-specific SaaS software to a vertical market

2000 components in code

200 developers

Introducing Black Duck to handle compliance

Internally generated need, but starting to get questions from customers.

Ongoing

## B2M Solutions

Providing management software and services to help companies manage their estate of mobile devices

Customers include big UK companies, and resellers include Japanese mobile device providers (already OpenChain members)

Manual compliance: <100 components, around 15 developers.

# SUMMARY

Open source is widespread

Infringement risk is an important consideration in compliance, procurement and M&A

Risk can be assessed by analysing code and licensing

Risk can be managed by implementing a sensible open source inclusion and use policy - such as OpenChain

Adopting OpenChain conformance will increase efficiency in the supply chain.



OpenChain provides the framework for compliance:  
other projects address specific practical compliance issues:

SPDX - licence taxonomy

SW360 - licence compliance project and catalogue management

FOSSology - licence and attribution text scanning and management

Quartermaster - dynamic tooling for licence compliance

 **OPENCHAIN**

**moorcrofts.com**

**orcro.co.uk**

**www.openchainproject.org**

