JBB

# Supplier License Compliance Audit (SLCA)

**Dr. Miriam Ballhausen**
Attorney at Law
JBB Rechtsanwälte, Berlin

OpenChain Conference Call| November 2nd, 2015

# Some Background Information

- Started working on the SLCA in the summer/ fall of 2014

- Goal: Draft a
  - questionnaire that
  - enables companies
  - using software supplied by third parties
  - in their products
  - to assess the open source license compliance
  - of their suppliers.

- Requirements
  - Easy to handle for suppliers.
  - Easy to handle for company conducting the audit.
  - Easy to handle for auditors.
  - Manageable results, even for companies that have many suppliers.

# Approach

- Team of lawyers and engineers
- Defined aspects/topics/areas companies need to audit.
- Drafted questions companies need to ask their suppliers related to these topics.
- Conducted test audits and revised the questions afterwards.
- Got involved in OpenChain.
- Have been revising our questions according to discussions/findings of the Open Chain group.

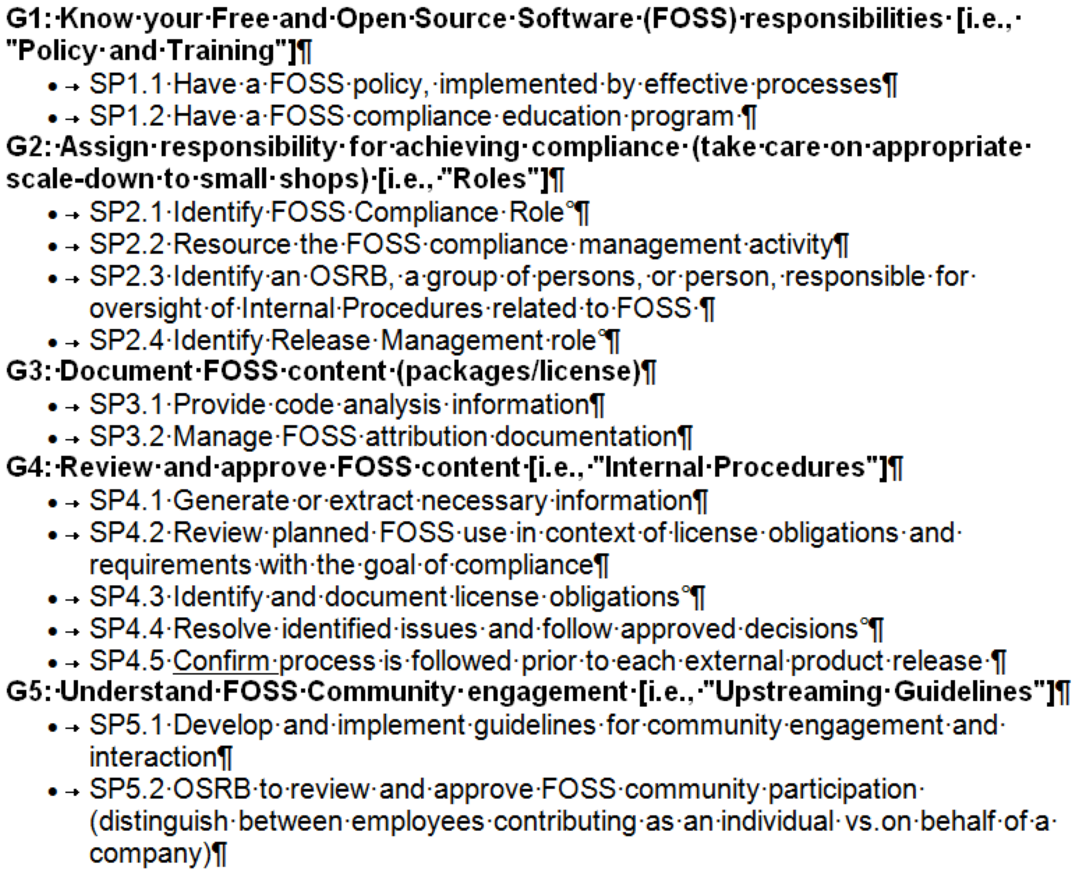
**Key Motivation: Don‘t design an audit that‘ll be run over once OpenChain is the standard.**

# Topics

- Organization
- Participation and Collaboration
- Incoming Code
- License Obligations
- Handling Copyleft Licenses
- Outbound Licensing and License Compatibility
- Maintenance Handling
- Patent Issues

# Topics

- Organization
- Participation and Collaboration
- Incoming Code
- License Obligations
- Handling Copyleft Licenses
- Outbound Licensing and License Compatibility
- Maintenance Handling
- Patent Issues



**G1: Know your Free and Open Source Software (FOSS) responsibilities [i.e., "Policy and Training"]**

- SP1.1 Have a FOSS policy, implemented by effective processes
- SP1.2 Have a FOSS compliance education program

**G2: Assign responsibility for achieving compliance (take care on appropriate scale-down to small shops) [i.e., "Roles"]**

- SP2.1 Identify FOSS Compliance Role°
- SP2.2 Resource the FOSS compliance management activity
- SP2.3 Identify an OSRB, a group of persons, or person, responsible for oversight of Internal Procedures related to FOSS
- SP2.4 Identify Release Management role°

**G3: Document FOSS content (packages/license)**

- SP3.1 Provide code analysis information
- SP3.2 Manage FOSS attribution documentation

**G4: Review and approve FOSS content [i.e., "Internal Procedures"]**

- SP4.1 Generate or extract necessary information
- SP4.2 Review planned FOSS use in context of license obligations and requirements with the goal of compliance
- SP4.3 Identify and document license obligations°
- SP4.4 Resolve identified issues and follow approved decisions°
- SP4.5 Confirm process is followed prior to each external product release

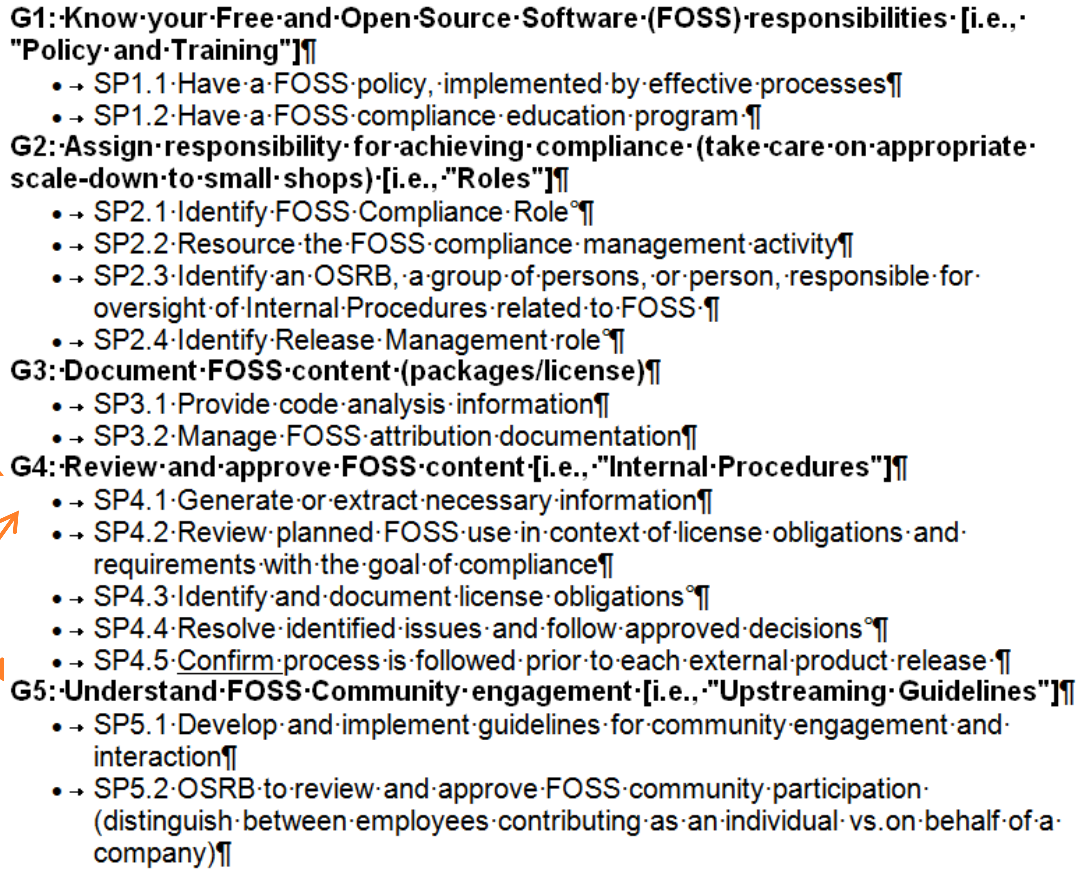
**G5: Understand FOSS Community engagement [i.e., "Upstreaming Guidelines"]**

- SP5.1 Develop and implement guidelines for community engagement and interaction
- SP5.2 OSRB to review and approve FOSS community participation (distinguish between employees contributing as an individual vs.on behalf of a company)

# Supplier License Compliance Audit

## Topics

- Organization
- Participation and Collaboration
- Incoming Code
- License Obligations
- Handling Copyleft Licenses
- Outbound Licensing and License Compatibility
- Maintenance Handling
- Patent Issues



**G1: Know your Free and Open Source Software (FOSS) responsibilities [i.e., "Policy and Training"]**

- SP1.1 Have a FOSS policy, implemented by effective processes
- SP1.2 Have a FOSS compliance education program

**G2: Assign responsibility for achieving compliance (take care on appropriate scale-down to small shops) [i.e., "Roles"]**

- SP2.1 Identify FOSS Compliance Role
- SP2.2 Resource the FOSS compliance management activity
- SP2.3 Identify an OSRB, a group of persons, or person, responsible for oversight of Internal Procedures related to FOSS
- SP2.4 Identify Release Management role

**G3: Document FOSS content (packages/license)**

- SP3.1 Provide code analysis information
- SP3.2 Manage FOSS attribution documentation

**G4: Review and approve FOSS content [i.e., "Internal Procedures"]**

- SP4.1 Generate or extract necessary information
- SP4.2 Review planned FOSS use in context of license obligations and requirements with the goal of compliance
- SP4.3 Identify and document license obligations
- SP4.4 Resolve identified issues and follow approved decisions
- SP4.5 Confirm process is followed prior to each external product release

**G5: Understand FOSS Community engagement [i.e., "Upstreaming Guidelines"]**

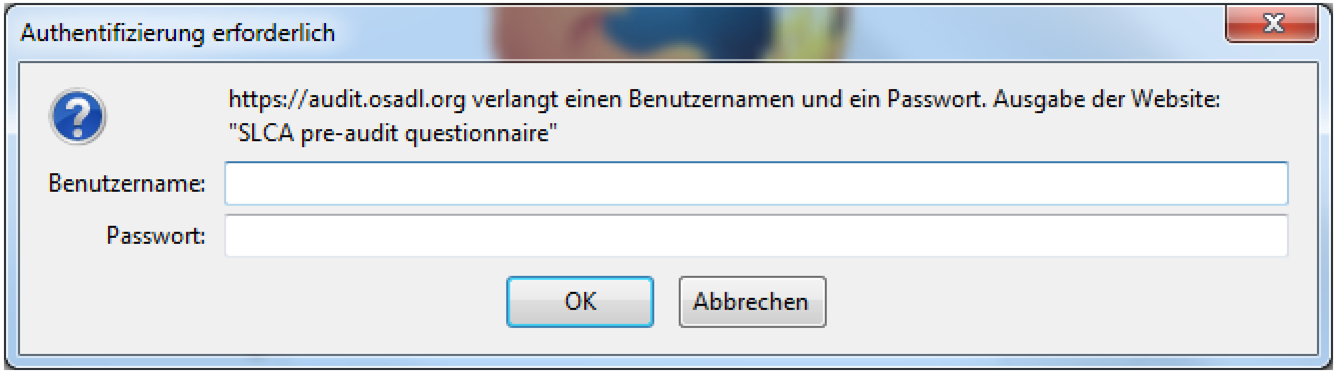
- SP5.1 Develop and implement guidelines for community engagement and interaction
- SP5.2 OSRB to review and approve FOSS community participation (distinguish between employees contributing as an individual vs.on behalf of a company)

# The Audit

- Set of questions designed for all types and sizes of suppliers.
- Questions asked depend on
  - Previous answers
  - Company size
- Efficient, as companies and auditors do not have to deal with questions/ answers that are irrelevant for the audit.

# Webbased Audit

- https://audit.osadl.org
- Requires user name and password.



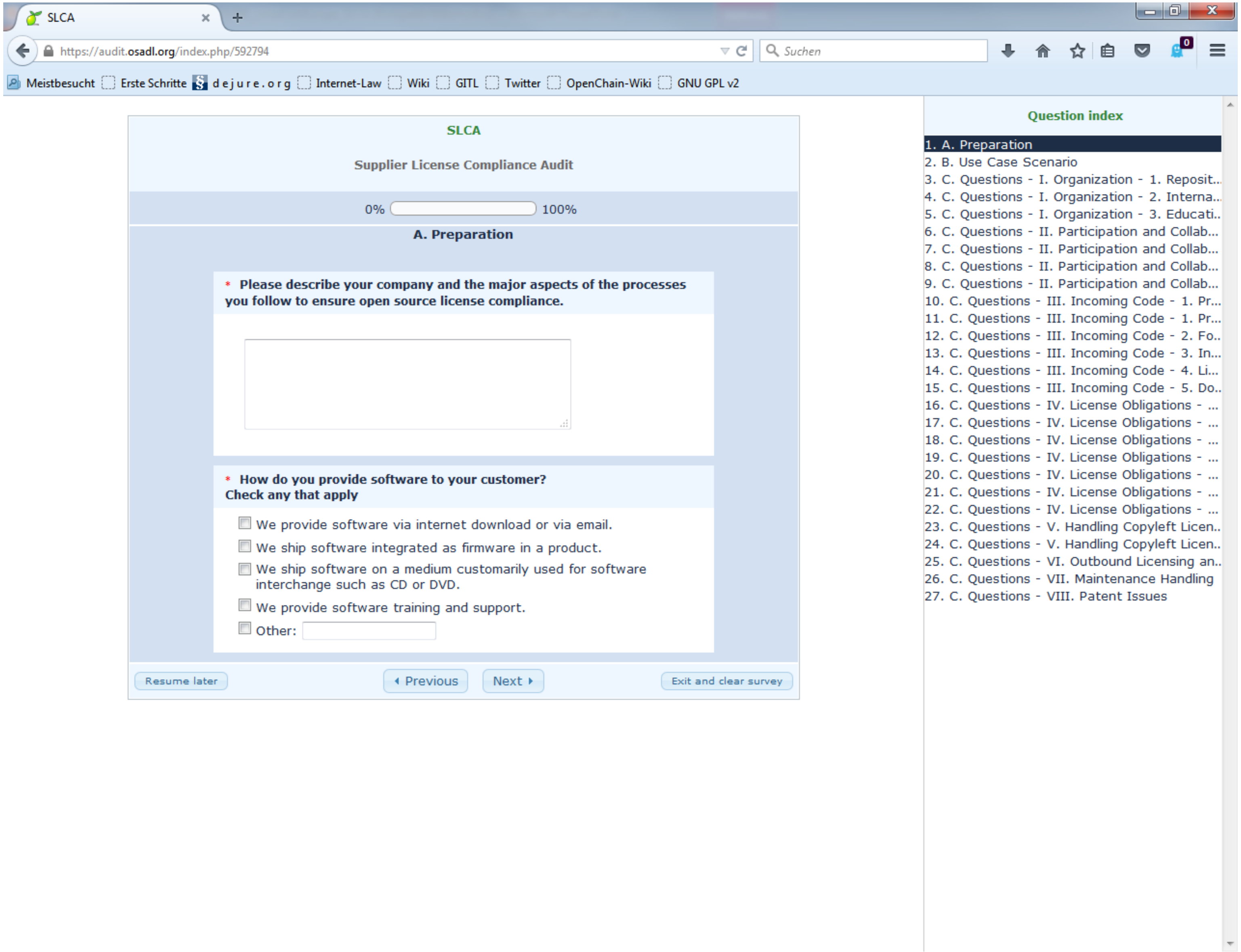
Authentifizierung erforderlich

https://audit.osadl.org verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "SLCA pre-audit questionnaire"

Benutzername:

Passwort:

# Supplier License Compliance Audit



**SLCA**

**Supplier License Compliance Audit**

0% 100%

**A. Preparation**

*** Please describe your company and the major aspects of the processes you follow to ensure open source license compliance.**

*** How do you provide software to your customer?**
**Check any that apply**

- □ We provide software via internet download or via email.
- □ We ship software integrated as firmware in a product.
- □ We ship software on a medium customarily used for software interchange such as CD or DVD.
- □ We provide software training and support.
- □ Other:

**Question index**

# The Test Audits

- Three test audits
- Three different types of companies:
  - Company that belongs to a group of companies and builds software/ software-tools for cars.
  - Middle-sized software outfit; FOSS is their standard.
  - Middle-sized supplier that just started to realize they have to deal with FOSS.
- Audit was manageable for all of them.
- Efficient, as companies and auditors do not have to deal with questions/ answers that are irrelevant for the audit.

# The Evaluation

- Mayor Challenge
- Auditors receive answers before the on-site audit.
- Contradictory answers are discussed during the on-site audit.
- The evaluation is based on the answers given during the online survey and the on-site audit.
- Apart from that the evaluation is still work in progress:
  - Effect of answers might depend on type and size of company
  - How can large numbers of suppliers be audited?
  - How can the audit results from large numbers of suppliers be evaluated?