SQS Services

sqs.com

LCM: License Compliance Management

Safeguard your products against the effects of the illicit use of Open Source Software

Are you compliant?

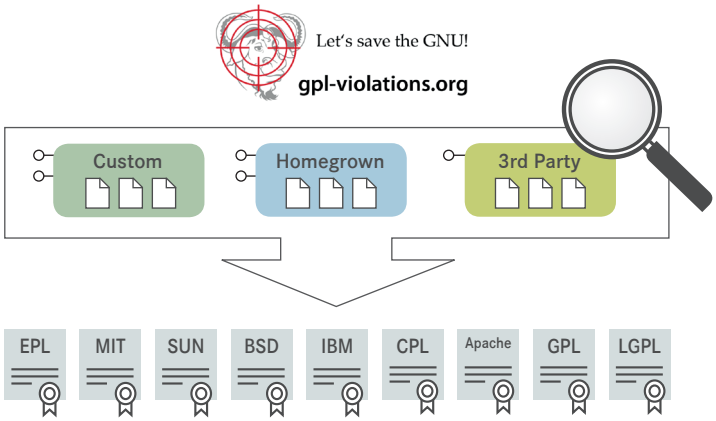
Unauthorized and unstructured usage of Open Source Software in commercial applications endangers the commercial success of many projects. How about you?

Lawsuits concerning the infamous **Intellectual Property** have recently gained public notoriety, partly due to their length and their high costs to all parties. At the same time, Open Source activists have joined forces, taking matters into their own hands and starting to prosecute alleged infringements of their rights.

What is the danger?

Four reasons, why the unchecked use of Open Source code is a dangerous and expensive undertaking:

- **Missing Awareness**
  Nowadays almost every software system makes use of the virtually ubiquitous amount of high quality Open Source software.
- **“Free” ≠ Free!**
  Using Open Source does not mean that licensed code can be used at will. The conditions of some licenses are surprisingly very restrictive.
- **GPL is viral**
  Particularly the most used GNU General Public License carry provisions that require code linked against GPLed code to be under the GPL as well – and forces the disclosure and publishing of the code.
- **Obligations vs. Strategy**
  Some Open Source license obligations routinely conflict with the intended purpose of commercial products!



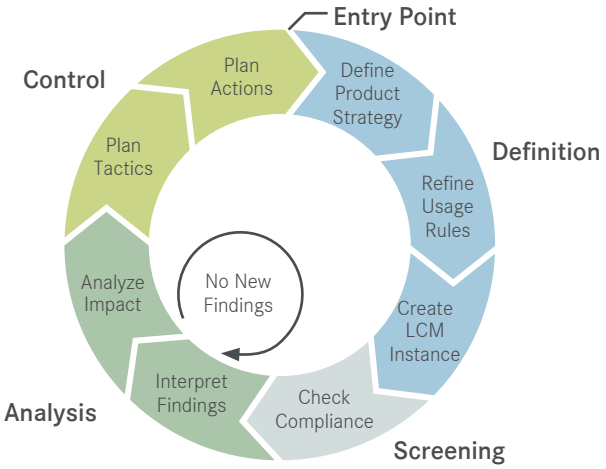
Safeguard yourself!

LCM use-cases:

- Use LCM for Risk-Management: Get **maximum transparency** about your Open Source usage and its impact for the project.
- Use LCM for the reliable estimation of the **unique value of software** and systems of a company when planning a merger or acquisition.
- Use LCM for outsourcing: Integrate it into SLAs and **check every delivery.**

The LCM Process

SQS provides you with a comprehensive process for License Compliance Management for your applications and systems:



The initial setup phase consists of four steps:

- During the **Definition** step, a general strategy and usage rules concerning Open Source are developed and the LCM process itself is tailored to the organization and its other processes.
- In a second step, called **Screening,** the compliance status of the existing application base is assessed.
- Afterwards, in the **Analysis** step, the findings of the compliance assessment are interpreted and their impact on the compliance of the system as a whole is analyzed. This step considers a 650+ of different licenses and their characteristics.
- The fourth and final step, **Control,** entails planning immediate responsive actions as well as corrections to the strategic decisions made in step one.

After the successful instantiation of LCM within your organization the focus is set on continuously managing and checking new versions for compliance. This last step can be fully automated and integrated into the software development and delivery process (e.g. as a nightly check run). Monitoring of the license compliance of your applications can be performed continuously.

The Black Duck Suite

The **Black Duck Suite** is an advanced enterprise-class solution to the unique management, compliance and security challenges associated with open source. It brings together the Black Duck Code Center, Export and Protex products into a unified framework. The Black Duck Suite automates key processes related to open source code management over the application development (AppDev) life cycle–search, select, approve, validation and ongoing monitoring.

Code Center supports the front-end of the development process where developers search for, select and obtain approval of open source components, as well as the ongoing monitoring of the components in use.

Protex and **Export** are used on the back end of the process when code needs to be validated before it is deployed.

The foundation of the Black Duck Suite is the **Black Duck KnowledgeBase.** Black Duck adds new code and new projects to the KnowledgeBase on an on-going basis. KnowledgeBase updates can incorporate hundreds or thousands of new project updates. This enables Black Duck customers to maintain currency with the dynamic open source community. KnowledgeBase updates are tested for accuracy before they are released to our customers.

Black Duck KnowledgeBase facts:

- Tens of billions of lines of code
- 475,000 + OSS projects, all versions
- From over 5,060 sites
- Representing 2,000 + unique licenses
- Covers 46,000 + security vulnerabilities
- 550 + cryptographic algorithms
- 7.8 billion code “fingerprints”

Contact

Do you have any questions or do you need more information? Please do not hesitate to send an e-mail: info@sqs.com