

Open Source License Compliance Report

SBOM Analysis & Commercial Use Assessment

Executive Summary

Compliance Status: **Conditionally Compliant**

This software is built on an open source foundation and

can be used legally in a commercial enterprise context, provided certain obligations are met. The majority (69.5%) of components use highly permissive licenses (Apache, MIT, BSD) that impose minimal restrictions. However, approximately 31% of components use copyleft licenses (GPL and LGPL) that require careful compliance procedures.

Key Findings:

- **85% of licenses permit unrestricted commercial use** (Apache, MIT, BSD, Public Domain)
- **15.7% GPL licenses** require source code disclosure if distributed
- **15.4% LGPL licenses** allow proprietary use with dynamic linking
- No copyleft requirements for internal enterprise use without distribution

License Distribution Analysis

Analysis of 338 software packages revealed the following license distribution:

License Family	Packages	Percentage
Apache (ASL 2.0, Apache-2.0)	120	35.5%
GPL (GPLv2, GPLv3)	53	15.7%
LGPL (LGPLv2+, LGPLv3+)	52	15.4%
MIT	47	13.9%
BSD	19	5.6%
Public Domain	14	4.1%
Eclipse (EPL)	10	3.0%
Other (MPL, ISC, Python, etc.)	23	6.8%

Detailed License Analysis

Apache License 2.0 (35.5% of components)

Commercial Compliance: Fully Compliant

The Apache License is a permissive license that explicitly allows commercial use without restriction. It is one of the most business-friendly open source licenses available.

Key Permissions:

- Unlimited commercial use and distribution
- Modification and creation of derivative works
- Patent grant protection from contributors
- Can be combined with proprietary code

Obligations:

- Include copy of the license with distributed software
- Retain copyright notices in source code
- Document any modifications made (if distributing)
- No requirement to release source code of your own software

MIT License (13.9% of components)

Commercial Compliance: Fully Compliant

The MIT License is one of the most permissive licenses available, requiring only minimal attribution.

Key Permissions:

- Unlimited commercial use
- Modification, distribution, sublicensing
- Can be incorporated into proprietary software

Obligations:

- Include copyright notice and license text
- No obligation to share modifications or source code

BSD License (5.6% of components)

Commercial Compliance: Fully Compliant

BSD licenses are highly permissive and similar to MIT, with minimal restrictions on commercial use.

Obligations:

- Retain copyright notice and license text
- 3-Clause BSD: Do not use author names for endorsement

GPL (General Public License) (15.7% of components)

Commercial Compliance: Conditional

GPL is a strong copyleft license. Commercial use is permitted, but requires careful compliance with distribution requirements.

Key Points:

- **Internal use is unrestricted** - No obligations if software is not distributed
- Commercial use and sale is explicitly permitted
- **Distribution triggers obligations** - Must share source code under GPL
- Derivative works must also be GPL-licensed

Compliance Strategies:

- **Option 1: Internal use only** - Use GPL software internally without distribution
- **Option 2: Separate executables** - Run GPL components as separate programs
- **Option 3: Dual licensing** - Obtain commercial license from copyright holder
- **Option 4: Full compliance** - Release your software under GPL with source code

LGPL (Lesser General Public License) (15.4% of components)

Commercial Compliance: Mostly Compliant

LGPL is a weak copyleft license specifically designed to allow use in proprietary software through dynamic linking.

Key Points:

- **Proprietary software can use LGPL libraries**
- Dynamic linking preserves proprietary code status
- Modifications to LGPL libraries must be shared
- Your own code remains proprietary

Obligations:

- Provide source code of LGPL libraries (including any modifications)
- Allow users to replace LGPL libraries with modified versions
- Include license and copyright notices
- Dynamic linking recommended (static linking increases obligations)

Your Compliance Obligations

For Internal Enterprise Use (No Distribution)

Status: Minimal Obligations

If you are using this software internally within your company without distributing it to customers or external parties, your obligations are minimal:

- **No source code disclosure required**
- No GPL/LGPL obligations trigger
- Maintain internal records of licenses used
- Comply with any internal corporate policies

For Distribution to Customers or External Parties

Status: Active Obligations

If you distribute this software to customers or external parties, you must:

For ALL Components:

- Include all applicable license texts
- Maintain copyright notices
- Provide attribution as required

For GPL Components (15.7%):

- **Critical:** Make complete source code available
- Include all GPL license texts
- Ensure derivative works are also GPL-licensed
- Provide written offer for source code if not included with distribution

For LGPL Components (15.4%):

- Provide source code of LGPL libraries (including modifications)
- Allow users to replace LGPL libraries
- Your proprietary code remains protected (if dynamically linked)

Recommendations

Immediate Actions

- **Document your use case** - Clarify if the software is for internal use or external distribution
- **Establish compliance procedures** - Create processes for license management
- **Archive license texts** - Maintain copies of all applicable licenses
- **Train development teams** - Ensure teams understand license obligations

Long-term Strategy

- **Implement automated license scanning** - Use tools to track licenses in dependencies
- **Consider license policy** - Define acceptable and restricted licenses for your organization
- **Evaluate GPL alternatives** - Consider replacing GPL components with permissive alternatives if distribution is planned
- **Seek legal counsel** - Consult with IP attorneys for complex scenarios

Conclusion

This software can be used legally in a commercial enterprise context. The majority of components use business-friendly licenses that impose minimal restrictions. However, proper compliance procedures must be established, particularly for the GPL and LGPL components.

For internal enterprise use, you are legally compliant with minimal obligations. For distribution scenarios, you must implement proper license compliance procedures, particularly for GPL-licensed components.

***Disclaimer:** This report provides general guidance on open source license compliance and does not constitute legal advice. For specific legal questions or complex scenarios, please consult with a qualified intellectual property attorney who specializes in software licensing.*