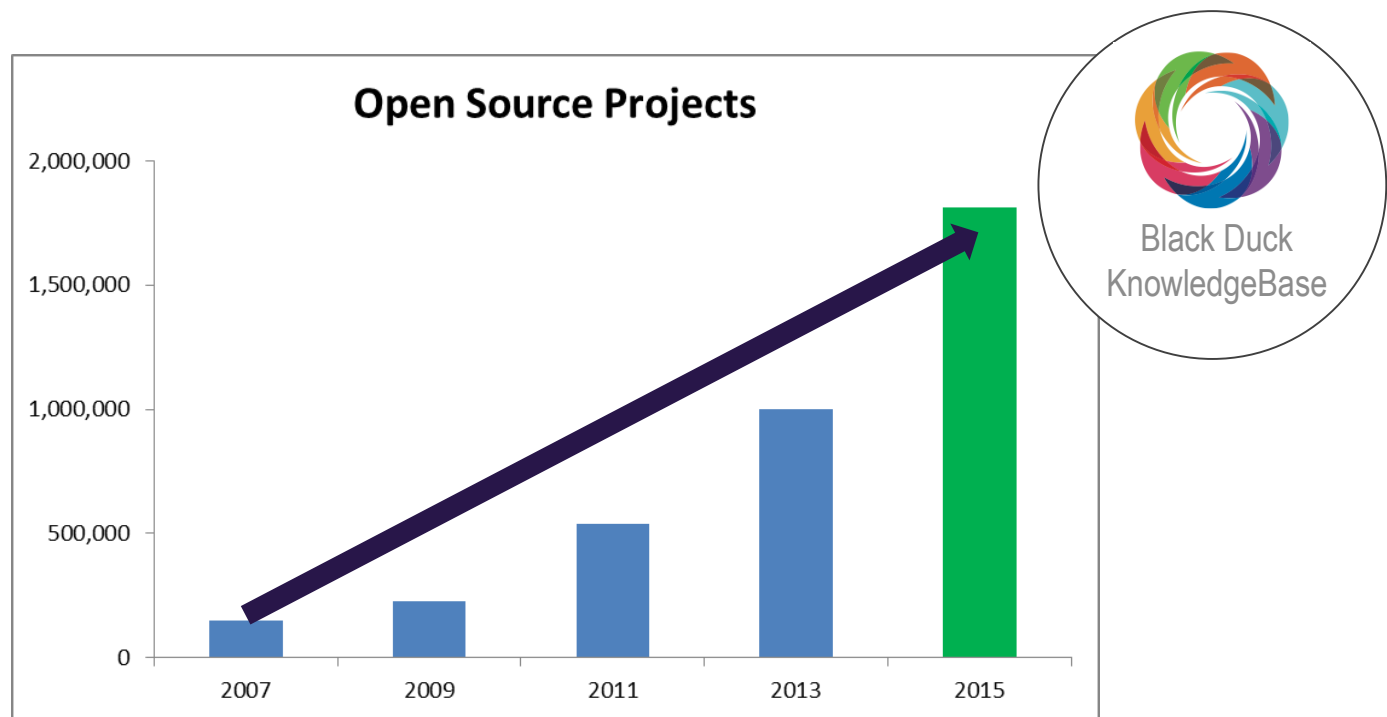# BLACK DUCK

Matthew H. Jacobs, Esq.

General Counsel, Black Duck Software, Inc.

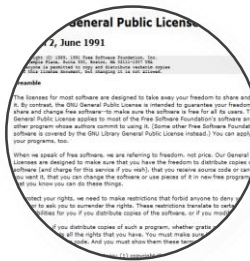# THE FOSS UNIVERSE IS EVER EXPANDING

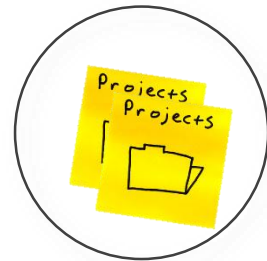

**Open Source Projects**


Black Duck KnowledgeBase

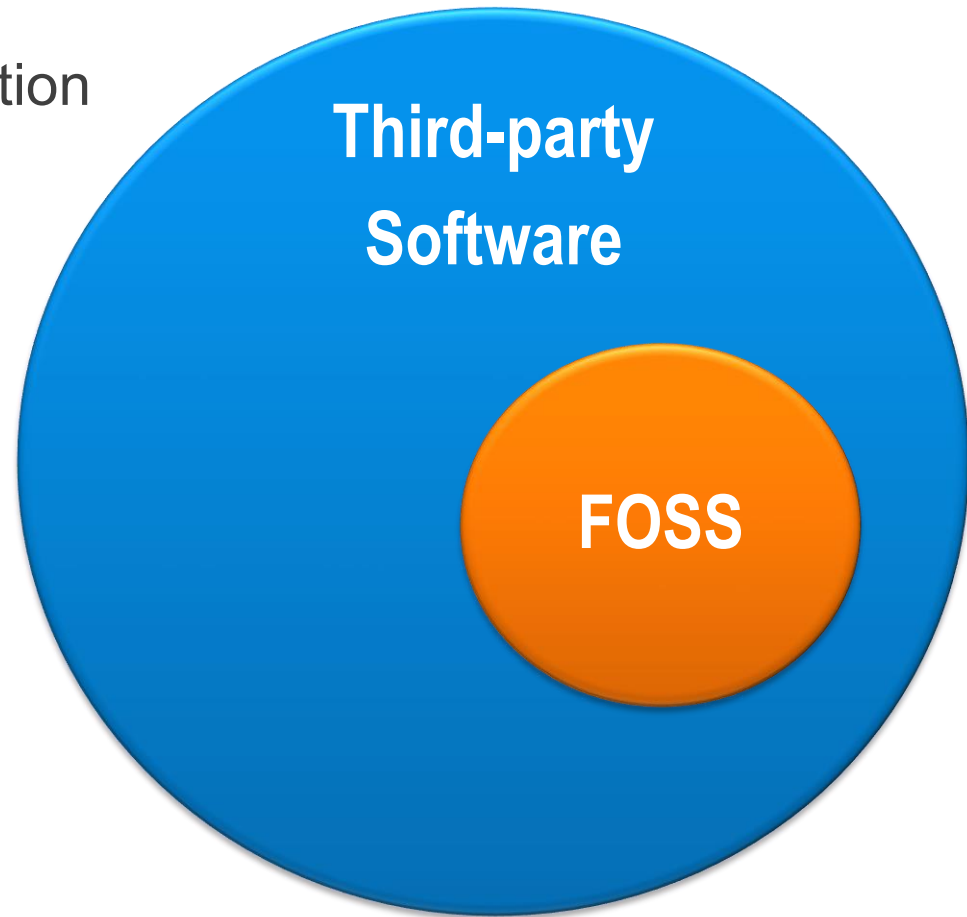**10+ Million** staff years

**>7,500+** sites

**2,300+** licenses

**4B+ files/1,000,000 +** unique projects

**BLACK**DUCK

# WHAT IS FOSS?

- It's third party software

- No single "official" definition

**BLACK**DUCK

# PRIMARY OSS LICENSE CATEGORIES

## Permissive Licenses (Academic)

- Licensee can use, copy, modify and distribute the software
- Licensee is allowed to combine the source with open source or proprietary software
- Licensee is NOT obligated to distribute the source code of derivative works

- BSD
- MIT

## Copyleft Licenses (Viral, Reciprocal)

- Any Licensee modifications to the software (derivative works) must be **distributed** under the same reciprocal OSS license
- Copyleft licenses are substantially more complex than permissive licenses

- GPL
- AGPL
- MPL

*See* **www.opensource.org**

**BLACK**DUCK

# OSS – THE 4 FREEDOMS



1. The freedom to run the program, for any purpose.

2. The freedom to **study how the program works**, and adapt it your needs.

3. The freedom to redistribute copies so you can help your neighbour.

4. The freedom to **improve the program, and release your improvements to the public**, so the whole community benefits.

# OPEN SOURCE DEFINITION

## Open Source Definition

1. Free Redistribution
2. Program must include Source Code and must allow distribution in source code as well as compiled form.
3. Must Allow Modifications and Derived Works
4. Integrity of the Author's Source Code
5. No Discrimination Against Persons or Groups
6. No Discrimination Against Fields of Endeavor
7. Distribution of License – no additional license can be required of others who redistribute the program
8. License Must Not Be Specific to a Product
9. License Must Not Restrict Other Software
10. License Must Be Technology-Neutral – not predicated on any individual technology

## Who is the OSI (Open Source Initiative)?

The OSI are the stewards of the Open Source Definition (OSD) and the community-recognized body for reviewing and approving licenses as OSD-conformant.

**BLACK**DUCK

# OTHER *INTERESTING* FOSS LICENSES

- Beer-ware



**BEERWARE**

- Tofu

- Fender Stratocaster

- No-nuke

- Chicken Dance

**BLACK**DUCK

# TOP 20 OPEN SOURCE LICENSES

| Rank | License |
|------|---------|
| 1 | GNU General Public License (GPL) 2.0 |
| 2 | Apache License 2.0 |
| 3 | GNU General Public License (GPL) 3.0 |
| 4 | MIT License |
| 5 | BSD License 2.0 |
| 6 | Artistic License (Perl) |
| 7 | GNU Lesser General Public License (LGPL) 2.1 |
| 8 | GNU Lesser General Public License (LGPL) 3.0 |
| 9 | Eclipse Public License (EPL) |
| 10 | Code Project Open 1.02 License |
| 11 | Microsoft Public License |
| 12 | Mozilla Public License (MPL) 1.1 |
| 13 | Common Development and Distribution License (CDDL) |
| 14 | BSD 2-clause "Simplified" or "FreeBSD" License |
| 15 | Common Public License (CPL) |
| 16 | zlib/libpng License |
| 17 | Academic Free License |
| 18 | GNU Affero GPL v3 |
| 19 | Microsoft Reciprocal License (Ms-RL) |
| 20 | Open Software License (OSL) |

Ranked according to number of open source projects using the license:

- Top 10 licenses account for **93%**
- Top 20 licenses account for **97%**
- GPL family of  licenses account for **53%**



License Share

- Code Project Open 1.02 License 1%
- Eclipse Public License (EPL) 1%
- GNU Lesser General Public License (LGPL) 3.0 3%
- All Other 7%
- GNU Lesser General Public License (LGPL) 2.1 6%
- Artistic License (Perl) 6%
- BSD License 2.0 7%
- MIT License 11%
- GNU General Public License (GPL) 3.0 12%
- Apache License 2.0 13%
- GNU General Public License (GPL) 2.0 33%
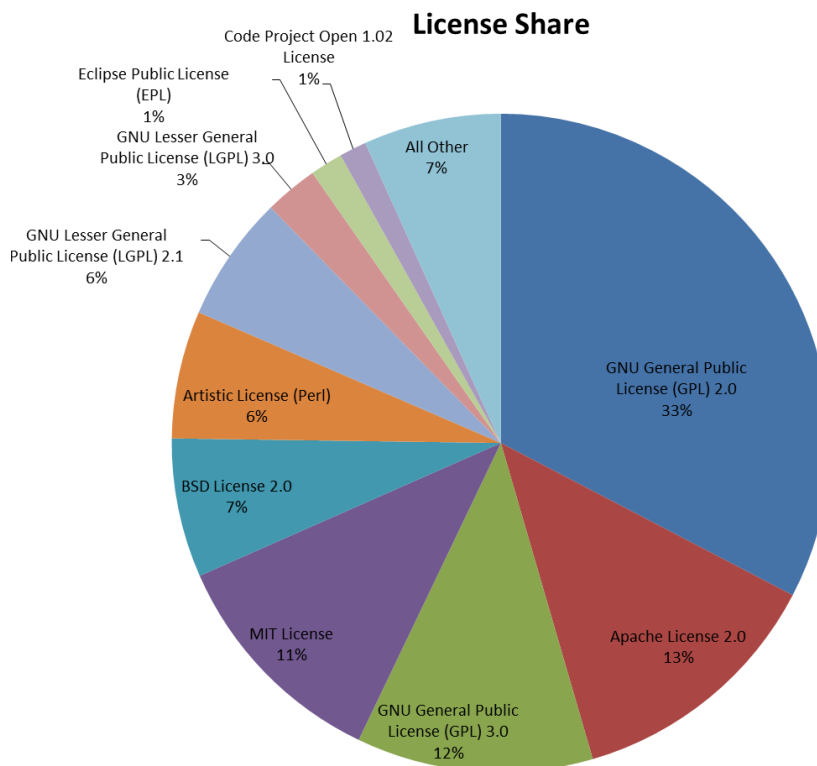
**Source**:  //www.blackducksoftware.com/oss/licenses#top20   April 2014

BLACKDUCK

# THE GOOD NEWS / BAD NEWS



Gartner Research
ID Number: G00210068
Publication Date: 24 January 2011

Survey Analysis: Overview of Preferences and Practices in the Adoption and Usage of Open-Source Software

Laurie F. Wurster, Bob Igou, Zeynep Babat

**Average Enterprise uses 29% open source code.**

**"50% of companies will face challenges due to lack of FOSS policy and management"**

**BLACK**DUCK

**"Over 80% of the software in our handsets is open source"**

Carl-Eric Mols, Head of OSS, Sony Mobile Communications

# MULTI-SOURCE DEVELOPMENT; CODE ENTERS A CODE BASE UNCHECKED



Open Source

Commercial 3rd Party Code

Code Base

Purchasing
- Licensing?
- Security?
- Quality?
- Support?

**SECURITY RISK**
Which components have vulnerabilities and what are they

**LEGAL RISK**
Which licenses are used and do they match anticipated use of the code

**OPERATIONAL RISK**
Which versions of code are being used, and how old are they

**BLACK**DUCK
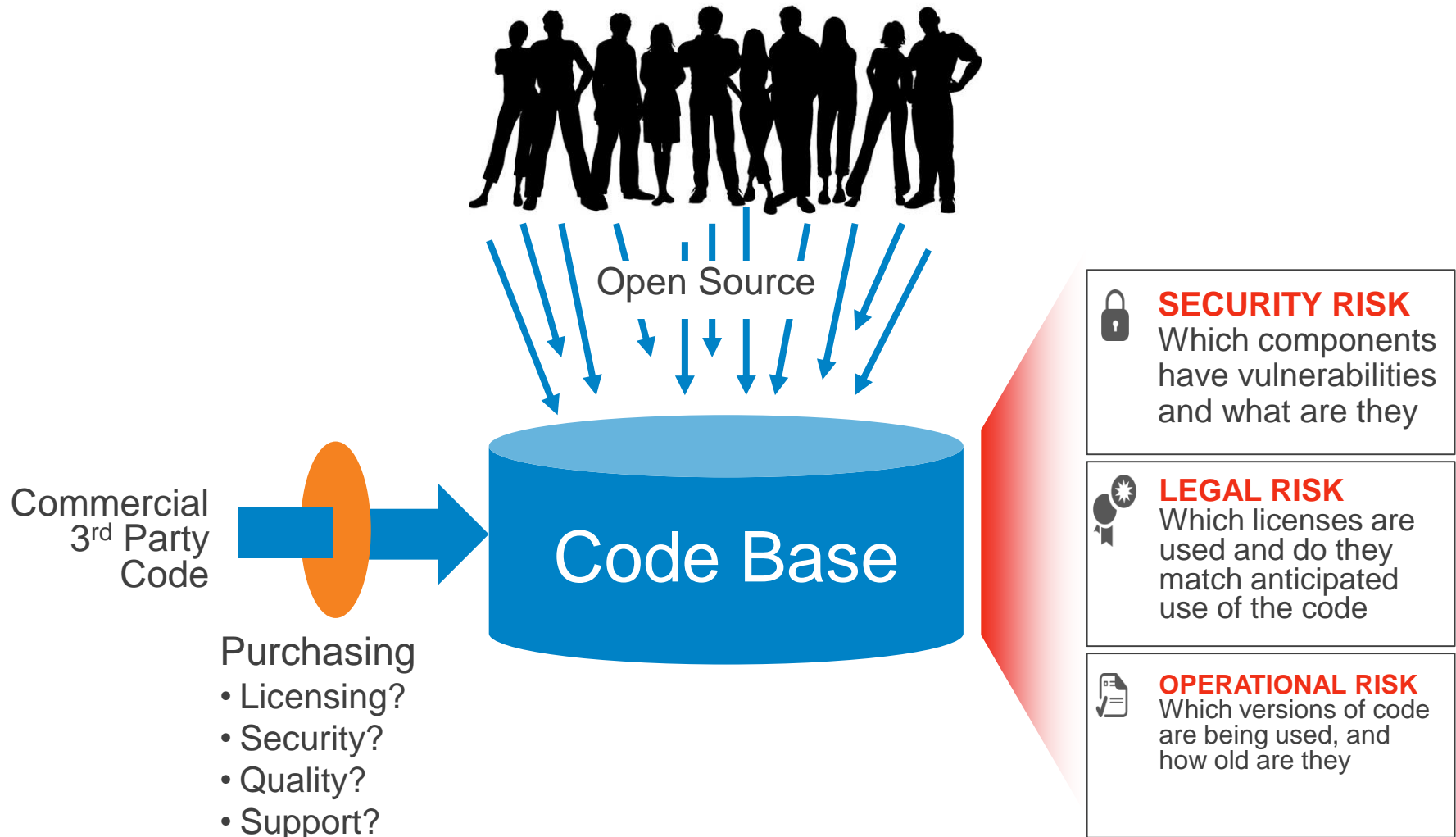
# OPEN SOURCE ADOPTION IN ENTERPRISE ORGANIZATIONS

A typical Enterprise IT organization has thousands of applications and uses hundreds of open source components

**Some apps Up to 90+% Open Source**

**ENTERPRISE AVERAGE 30%**



Third-party Commercial Code (10MB) 3%

Code Duplicated with Other Projects (18MB) 4%

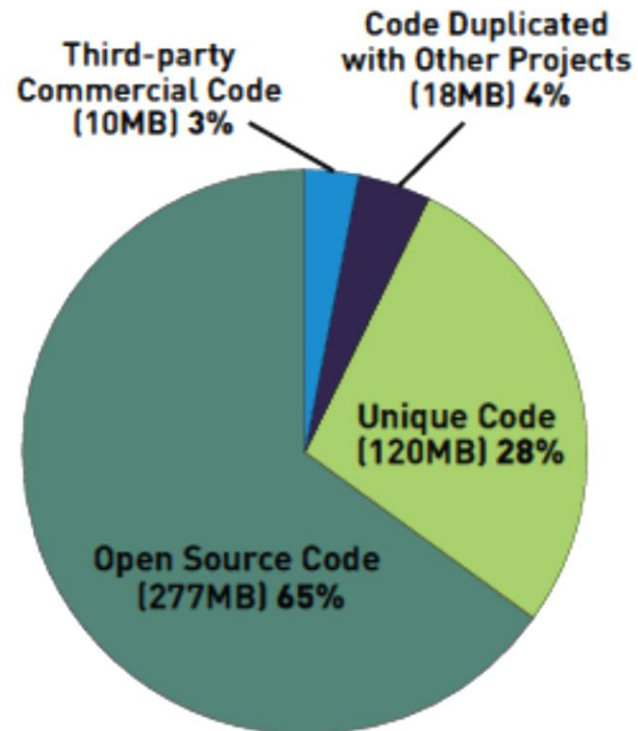Unique Code (120MB) 28%

Open Source Code (277MB) 65%

Fig. 1. Open source and Proprietary code base composition. UK Investment Bank Trading Application.

**BLACK**DUCK

# BLACK DUCK'S EXPERIENCE ANALYZING CODE

- 99% of code audits find open source.

- 95% of audits find <u>unknown</u> open source

- 75% of audits contain unknown licenses.

- 50% of code audits contain GPL.

- Audits on average contain 33% open source.

- 5% of M&A deals never materialize due to our findings
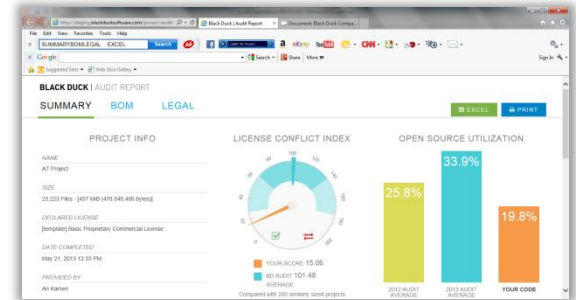
# WHY INVESTORS & ACQUIRERS CARE

- Investors and Acquirers are asking about OSS use & compliance

- Current Litigation: compliance is an important issue
  - Versata v. Ameriprise
  - Ximpleware v. Ameriprise

- M&A OSS Problems:
  - Longer/Larger Escrows
  - Purchase Price Erosion
  - Costly Remediation

**BLACK**DUCK