FOSS License Selection and Code Management

Peter Vescuso, Black Duck Software

EOLE 2011, Barcelona

November 4, 2011

Agenda

- FOSS trends
- Types of licenses
- Choosing a license
- FOSS management and compliance
- Summary

Market Trends

"Software is Eating the World"

Marc Andreessen

"Open source is ubiquitous, it's unavoidable….having a policy against open source is impractical and **places you at a competitive disadvantage"**

Mark Driver, Gartner

blackduck™

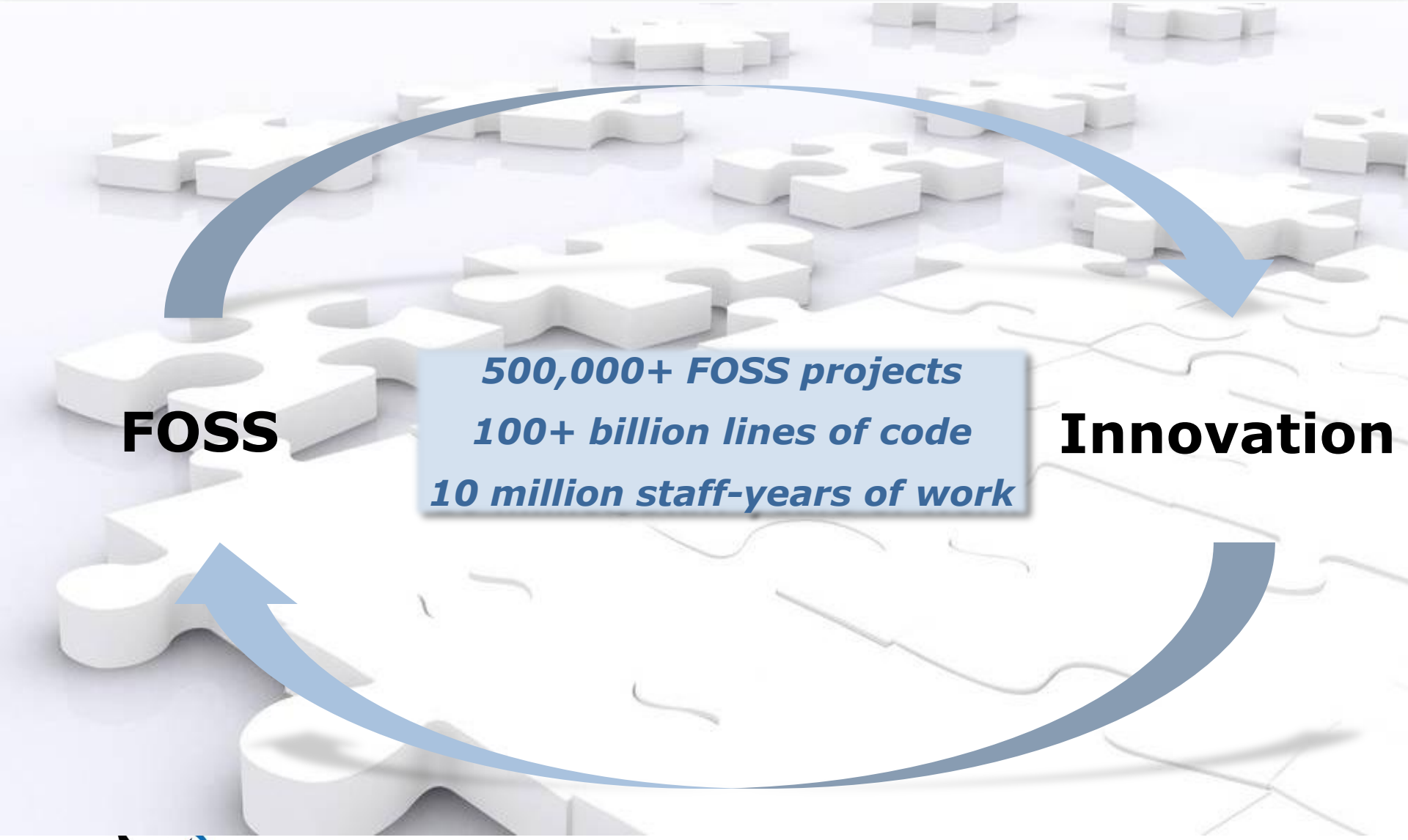
Know Your Code.®

FOSS: the Foundation for Game Changers

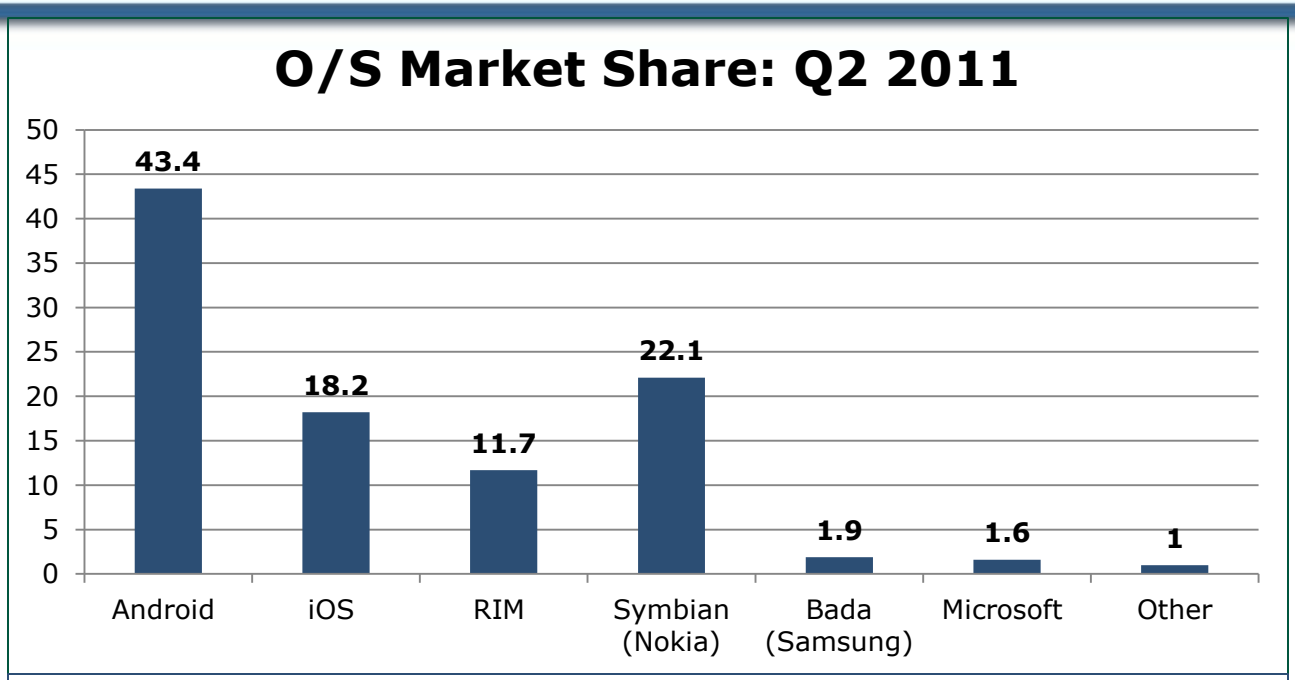
blackduck

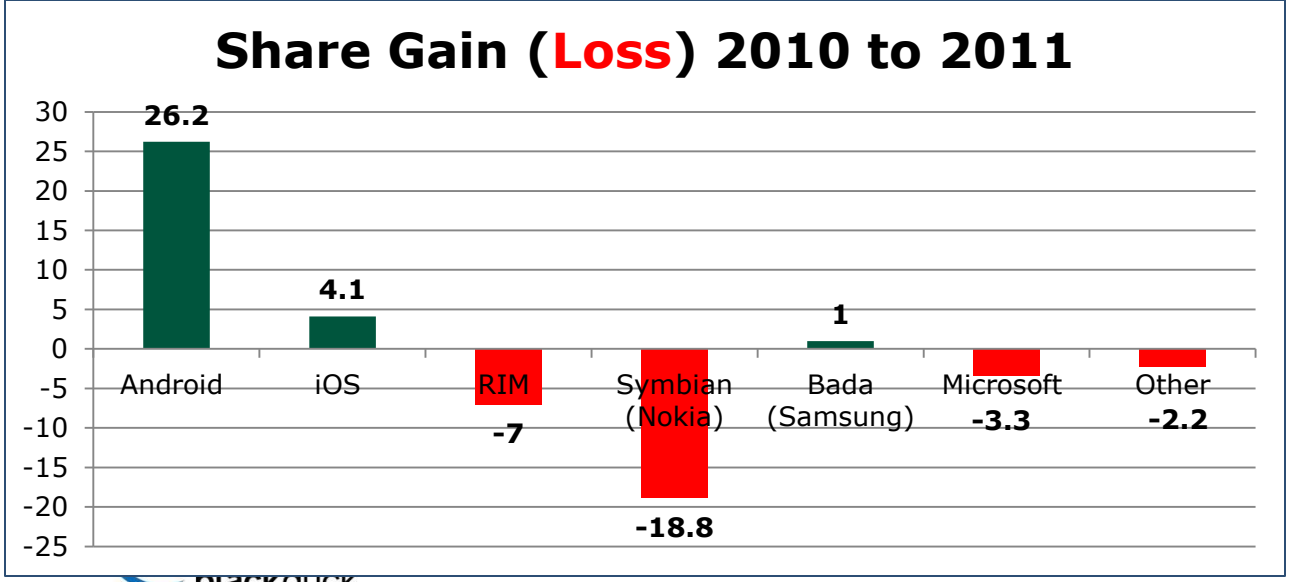
Know Your Code.

The Virtuous Circle – Innovation & FOSS



Open Source is a Large, Growing Opportunity





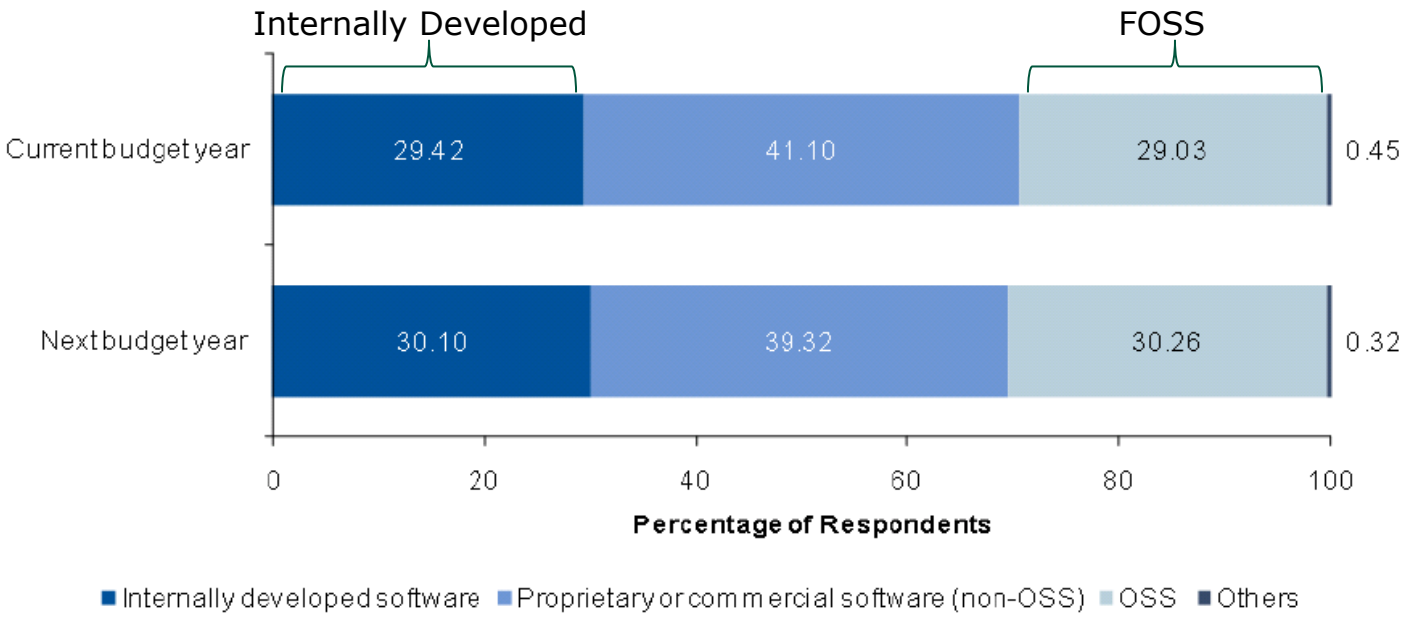
- 428.7 million units
- 16.5% growth form Q2 ’10

Source: Gartner , August 2011

FOSS Use = Internally Developed Code

- Gartner survey of 547 IT leaders reports that FOSS and internally developed code are equal (29%) in terms of deployed software

Figure 12. Structure of Deployed Software



Source: Overview of Preferences and Practices in the Adoption and Usage of Open Source Software, January 2011, Gartner Group

Challenges Using FOSS at Scale

For Developers

- Education and awareness about FOSS
- Making good decisions about which FOSS to use
- Wasted effort re-creating what already exists
- Maintaining FOSS deployed in apps/services

For Enterprises/Organizations

- FOSS strategy & policy
- Ensuring compliance
- Search, selection, validation

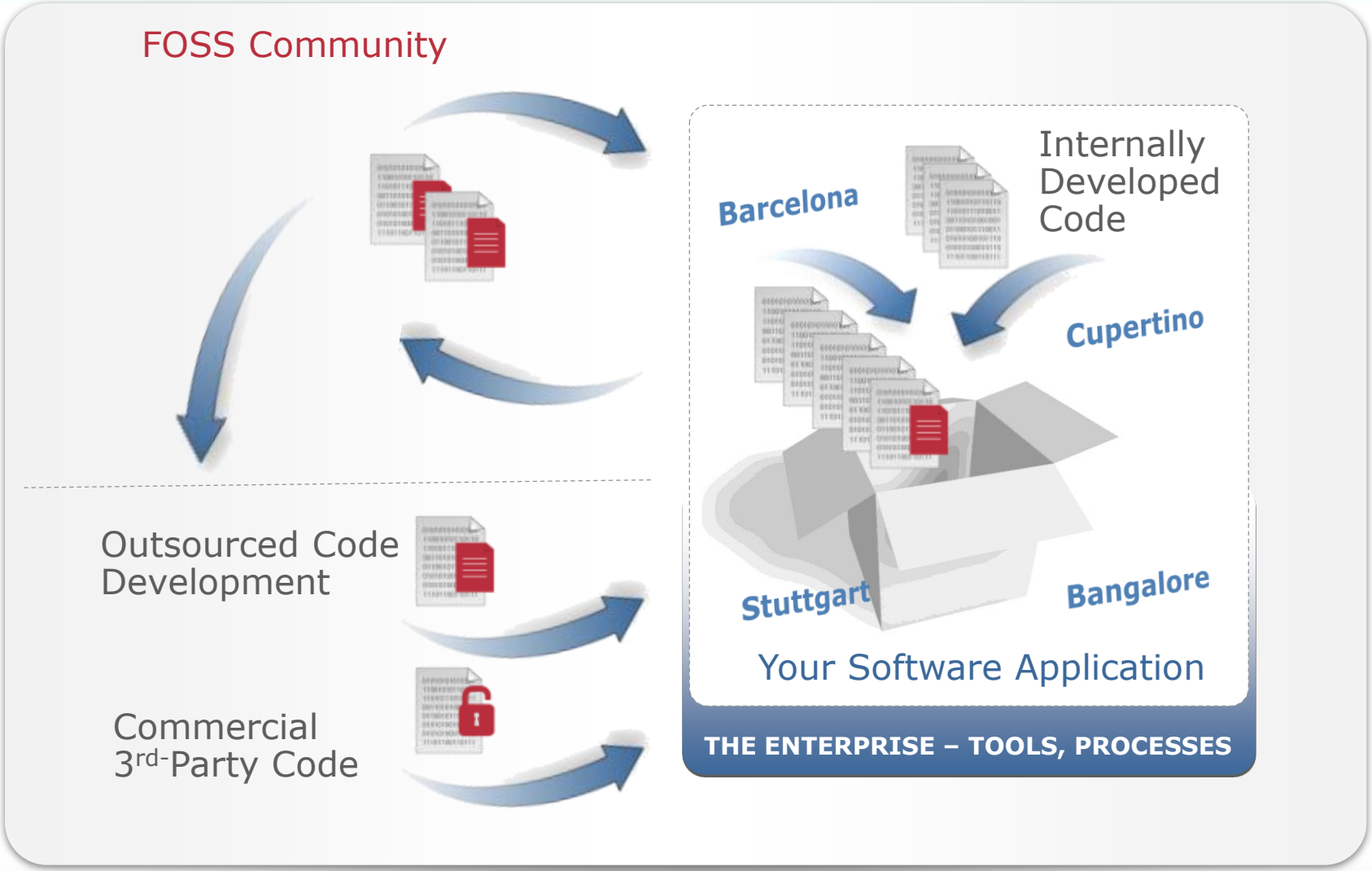
Gartner FOSS Analysis (Nov. 2010)

✓ 50% of the Global 2000 will face challenges due to lack of FOSS policy & management

blackduck™

Know Your Code.®

The Challenge of "Multi-Source" Development at Enterprise Scale



Know Your Code.®

IT Development Benefits and Challenges with Open Source

Gartner

- **Benefits**
  1. Flexibility
     - Modify, mix, reuse code
  2. Innovation
     - Leverage FOSS & community
  3. Cost optimization
     - Reduce or eliminate acquisition cost

- **Challenges**
  1. Technical failure
     - Operational exposure
     - Needs to be audited, managed
  2. Security risks
     - Business exposure
  3. IP Risks
     - Legal exposure

Source: Mark Driver, Gartner Group, November 2010.

blackduck™

Know Your Code.®

Agenda

- FOSS trends
- Types of licenses
- Choosing a license
- FOSS management and compliance
- Summary

OSI: Criteria for Open Source License

1. Free Redistribution
2. Provide Source Code
3. Allow 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
8. License Must Not Be Specific to a Product
9. License Must Not Restrict Other Software
10. License Must Be Technology-Neutral

blackduck™

Know Your Code.®

Types of Open Source Licenses: Restrictive vs. Permissive

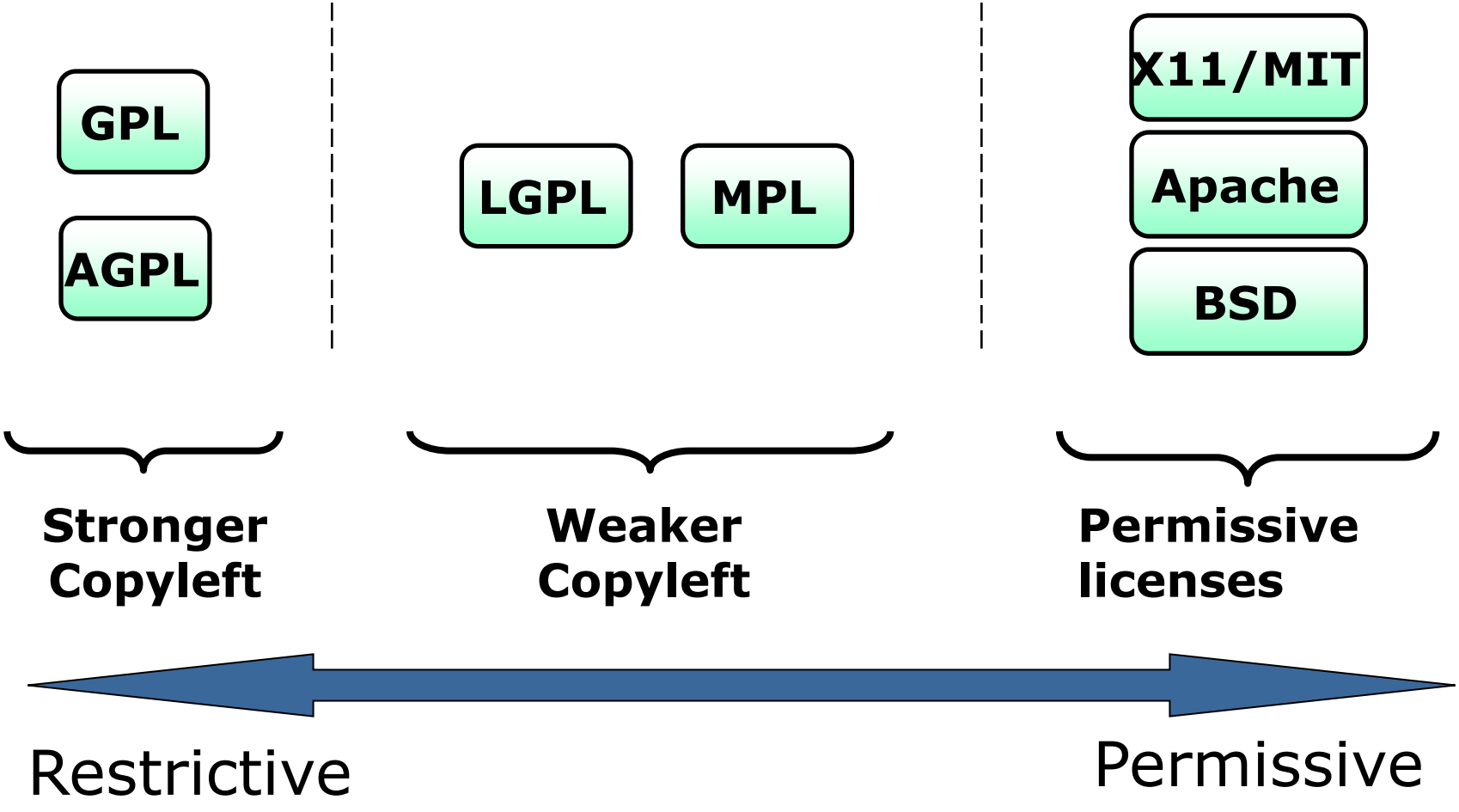
- **Restrictive (aka Copyleft, Reciprocal)**
  - Requires licensee to make improvements or enhancements available under similar terms
  - Example is the GPL: Licensee must distribute "work based on the program" and cause such works to be licensed at no charge under the terms of the GPL

- **Permissive**
  - Modifications/enhancements may remain proprietary
  - Distribution in source code or object code permitted provided copyright notice & liability disclaimer are included and contributors' names are not used to endorse products
  - Examples: MIT, BSD, Apache Software License

blackduck™

Know Your Code.®

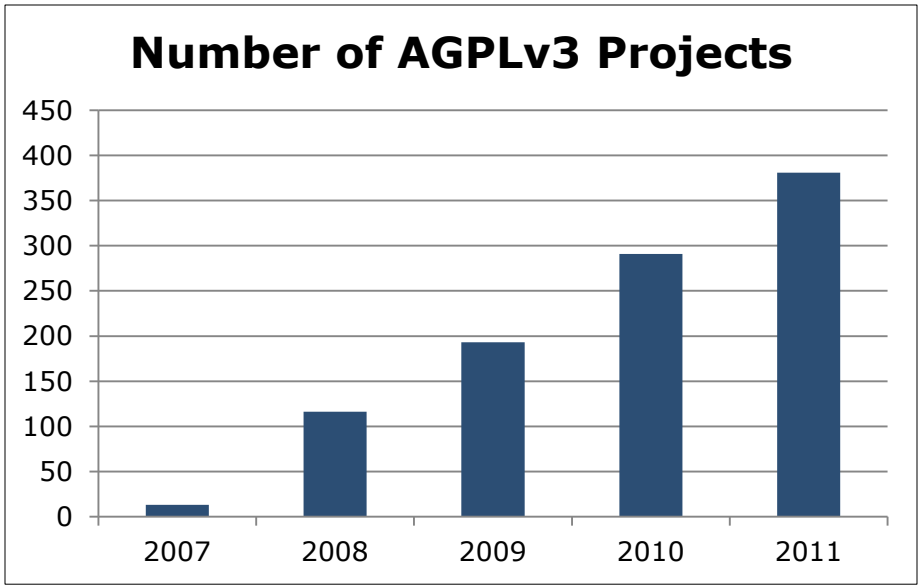
The OSS License Continuum



blackduck™

Know Your Code.®

Open Source Projects Available Under the AGPLv3



- Approaching 400 projects
- Growing at ~50% CAGR

Source: //www.blackducksoftware.com/osrc/data

SUGARCRM

FUNAMBOL

launchpad

DIASPORA*

status.net

GITORIOUS

OpenERP
OPEN SOURCE BUSINESS APPLICATIONS

PHP-FUSION

blackduck

Know Your Code.

The Beer License

<phk@FreeBSD.ORG> wrote this file. As long as you retain this notice you can do whatever you want with this stuff.

If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

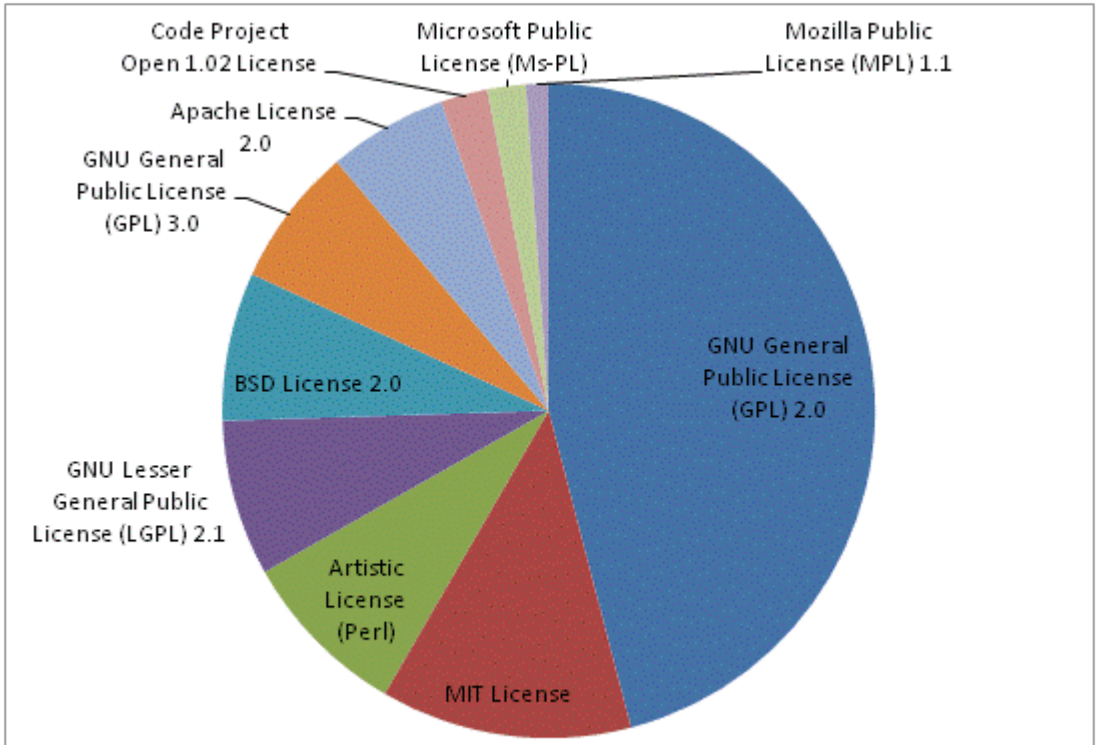
blackduck™

Most Popular Open Source Licenses

Top 20 Licenses

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

Share of Top 10 Licenses



- Ranked according to number of FOSS projects using the license
- Top 10 licenses account for **93%**
- Top 20 licenses account for **97%**
- GPL + LGPL licenses account for **57%**

Source: http://osrc.blackducksoftware.com/data/licenses/

Golden Rules

"Honor intellectual property rights"

"Do the 'right' thing -- comply with the author's wishes"

blackduck™

Know Your Code.®

Open Source Myths*

- You cannot use open source software in a proprietary environment [or you will die]
- All open source licenses require the release of source code for everything
- The easiest answer is to "just say no"
- None of these agreements are enforceable so it doesn't really matter anyway
- No one will ever know
- Our corporate policy says we don't use open source

*Source: Karen Copenhaver; Choate, Hall & Stewart

blackduck™

Know Your Code.®

Considerations for Choosing a License

Author/Licensor

- Want to maintain control?
  - No, then liberal licenses such as MIT or BSD can be preferable to "public domain"
  - Yes, see below
- Do you want enhancements made available to the community?
  - Yes, use a reciprocal license
  - No, use a permissive license
- Do you want to receive license fees?
  - Dual license is possible
    - MySQL and Pentaho use both GPL and commercial licenses
- Hosted service?
  - Consider AGPL (e.g., SugarCRM, Funambol, OpenERP, 400 others)
- Avoid license proliferation – only use OSI approved

User/Licensee

- Want to maintain control of your enhancements?
  - No, use reciprocal or permissive
  - Yes, use permissive licenses
- Warranty and indemnification
- License requirements, e.g.,
  - Make improvements available
  - Identify contributors
  - Include copyright notices
  - Include copy of the license agreement

blackduck™

Know Your Code.®

Potential License Conflicts

- Proprietary licenses.
  - Pay a fee
  - Can’t reverse engineer
- Many FOSS licenses allow restrictions on end users (Apache 2), but GPL does not.
- Some FOSS licenses contain patent termination clauses.
- Apache and GPLV2 were incompatible, but GPLV3 resolved it

blackduck™

Know Your Code.®

Agenda

- FOSS trends
- Types of licenses
- Choosing a license
- FOSS management and compliance
- Summary

blackduck™

Know Your Code.®

What I Hear from Development Managers

- "We have little to no visibility into the FOSS used in our projects."
- "I'm accountable for all of this and I have little control."
- "Our open source policies will slow down our development schedules."
- "It's difficult to support applications that contain open source code."
- "It's hard to get developers to comply with our open source policies."
- "We don't have an open source strategy, or policy and processes in place."

blackduck™

Know Your Code.®

Requirements for FOSS Governance & Compliance

Strategy

- Articulate the business objectives for use of FOSS

Policy & Process

- FOSS policy & management process

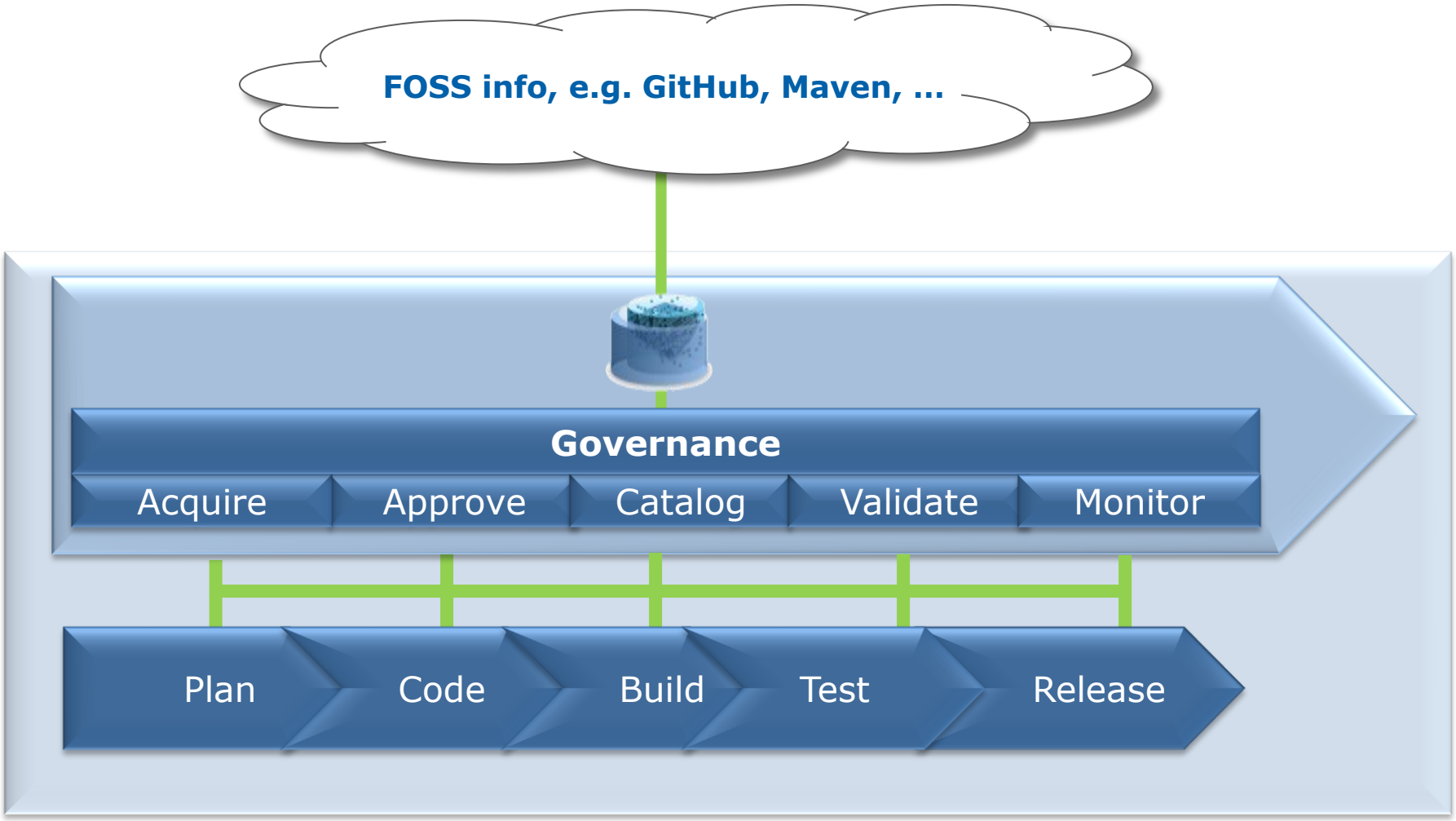
Technology

- Automate governance and compliance
- "Design-in" and automate policies

blackduck™

Know Your Code.®

Ensuring Compliance Across the Lifecycle



blackduck™

Know Your Code.®

Managing FOSS & Ensuring Compliance

Know Your Code.®

Managing FOSS & Ensuring Compliance

Acquire ▶ Approve ▶ Catalog ▶ Validate ▶ Monitor

Search for code,

Select code based on policies and metadata

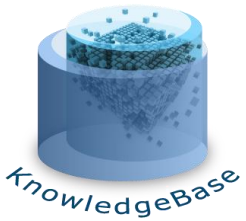
Review & Approve Review and approve code based on policies

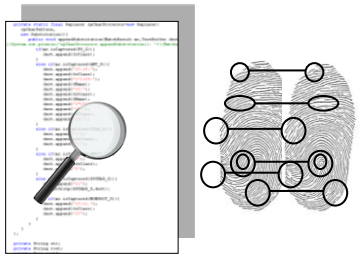
Catalog & Index

Build and publish a catalog

Analyze & Audit code so that only authorized code is used

Monitor & Maintain code usage and impact across applications





blackduck™

Know Your Code.®

Software Package Data Exchange™ (SPDX™)

- Working group of the Linux Foundation
- Charter:
  - Create data exchange standards to enable license and component information sharing (metadata)
- Broad industry support
- V1,0 released in August 2011

"SPDX is a crucial building block in an industry-wide system of automated license compliance administration"
Eben Moglen, SFLC

blackduck™

Know Your Code.®

Summary

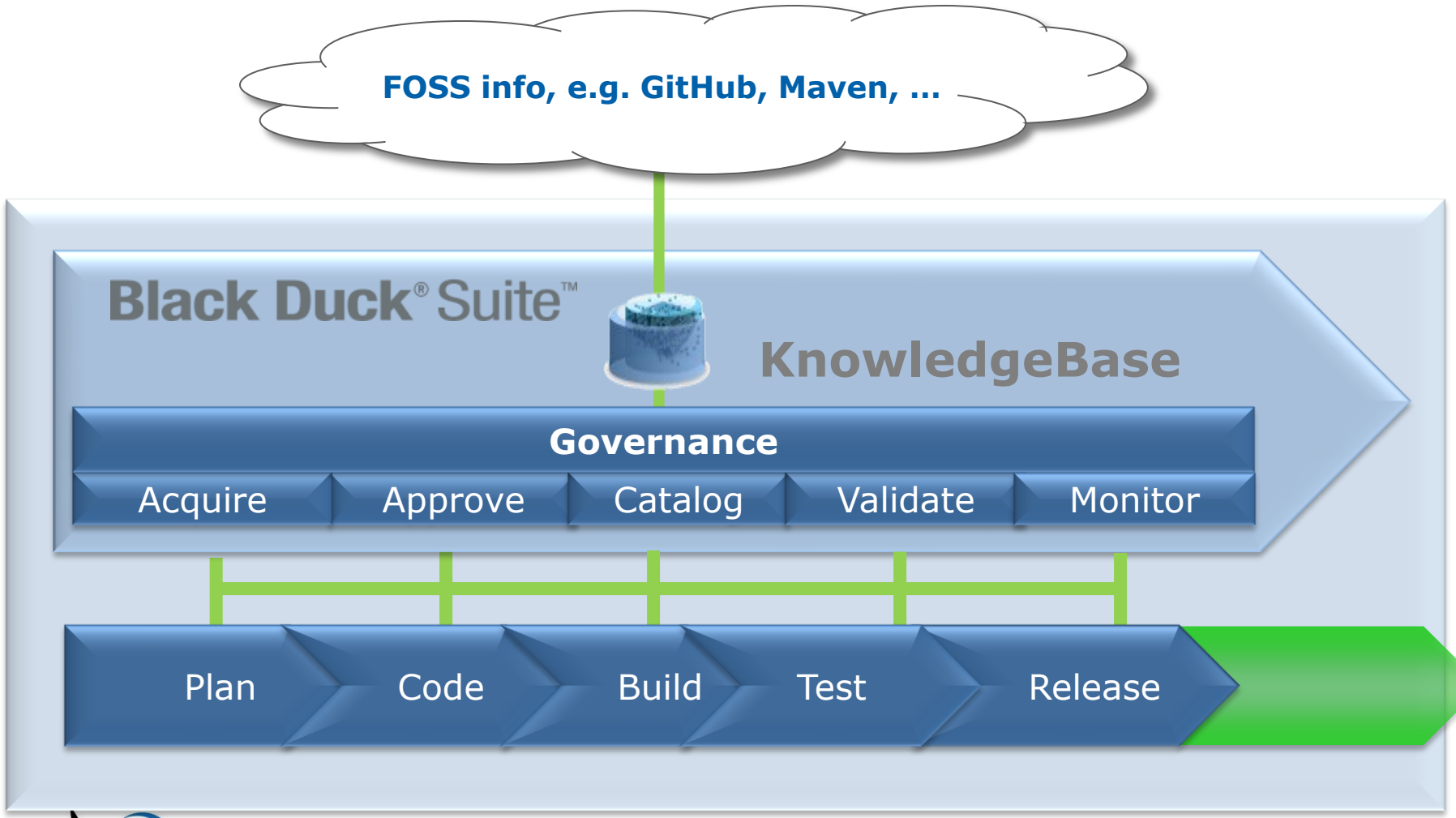
- FOSS is changing the world
  - It's ubiquitous and an essential element of software strategy
  - Development process with FOSS is different….
- Choosing a FOSS project requires both legal and technical evaluation
  - Must understand the obligations you are assuming
- Realizing the full benefits and ensuring compliance requires an explicit statement of strategy/policy combined with the right tools and automation technology

blackduck™

Know Your Code.®

About Black Duck Software

Build better software faster by automating and managing the acquisition and governance of open source



blackduck™

Know Your Code.®

Information Resources

- Webinars for Legal training
  - Introduction to Open Source Licenses
  - Understanding the Top 10 Open Source Licenses
  - Best Practices in Managing Open Source
  - Unraveling the Complexities of the GPL
  - And more….
  - **//www.blackducksoftware.com/webinars/legal/**
- SPDX
  - www.blackducksoftware.com/spdx/intro_to_spdx.mov
- M&A
  - Open Source Due Diligence in M&A and Financing
  - Technical Due Diligence for M&A: The Perspective from SAP
  - **//www.blackducksoftware.com/webinars/m-and-a/**
- Android white paper & webinar
  - **//www.blackducksoftware.com/android**
  - **//www.blackducksoftware.com/webinars/legal/android.html**
- Data: Open Source Resource Center (licenses, projects, languages)
  - **//osrc.blackducksoftware.com/**

blackduck™

Know Your Code.®

Black Duck Legal Specialist Certification

- Valuable Course
  - Become expert in the Black Duck approach to software assessment
    - Understand Problem, Process, Capabilities
  - Learn how to interpret details of Black Duck assessment reports
    - Add more value in assessing risk
  - Interact with Black Duck experts and peers
- Recognition of Expertise
  - Be associated with the #1 name in open source compliance
  - Receive visibility for you and your firm on the Black Duck website (optional)
  - Gain credibility with potential M&A clients

blackduck™

Know Your Code.®