FOSS in Financial Institutions

The Game has Changed

Claus-Peter Wiedemann
Senior Manager, FOSS Services, BearingPoint

FOSS CON Korea 2014
Seoul, December 4, 2014

BearingPoint®

Disclaimer

This presentation does NOT constitute Legal Advice. None of the information given herein may be relied upon in lieu of consultation with an appropriate lawyer specialized in Free & Open Source Software matters and qualified to give advice in the area of copyright law and other areas of law which this presentation may relate to.

BearingPoint

Gartner predicts…

By 2016, at least 95% of IT organizations will leverage nontrivial elements of open source software technology in their mission-critical IT portfolios, including cases where they might not be aware of it — an increase from 75% in 2010.

https://www.blackducksoftware.com/files/webmedia/_webinars/11-12-14_T.Rowe.pdf

… and Barclays Bank executes

Barclays claims 90 percent software cost savings with open source drive

http://www.v3.co.uk/v3-uk/news/2234593/barclays-slashes-software-spend-by-90-percent-with-open-source-drive

FOSS enables a financial institution to …

- … accelerate innovation
  - Reuse non-differentiating code
  - Utilize the power of communities
  - Enable/accelerate standardization
- … better fulfil regulatory requirements
  - Source code availability → see what the code (really) does
  - Code is deployed (and tested) by many and in other domains → higher code quality
- … attract top talent
- … bring software development productivity to the next level
- … save money

Business Risks of FOSS Deployment

- Technical
- Operational
- Security
- Legal

Business Risks of FOSS Deployment

Technical & Operational

- Unknown architecture
- Unknown code quality/documentation
- Unknown efforts for maintenance and support availability
- Unknown fitness for regulatory requirements
  - PCI-DCS
  - Sarbanes-Oxley
  - Basel II/III

Business Risks of FOSS Deployment

Technical & Operational

Mature financial institutions …

- … define technical entry gates for FOSS
- … consider community activity and other meta data
- … apply the same stringent quality assurance procedures to FOSS
- … actively participate in FOSS communities and contribute code
- … coordinate FOSS use across organizational boundaries

Use proper tooling. Manual attempts will fail.

Outsource to experienced supplier.

Business Risks of FOSS Deployment

Security

- Security is most critical for financial institutions
  - Regulatory requirements (e.g. PCI-DSS)
  - High damage potential (data and money loss)
  - Reputation damage can be detrimental to the business

- FOSS specific aspects
  - Source code is available → hard to hide malicious code
  - Vulnerabilities can get fixed (very) fast
  - Many different FOSS components are deployed in many products
  - Version proliferation (e.g. old, new versions mixed)
  - Own responsibility for finding out about security vulnerabilities

Business Risks of FOSS Deployment

Security

Mature financial institutions …

… keep track meticulously where which FOSS is deployed

… evaluate known security vulnerabilities when new FOSS is selected

… constantly monitor the FOSS communities and other public data sources for new security vulnerabilities

Use proper tooling. Manual attempts will fail.

Outsource to experienced supplier

Business Risks of FOSS Deployment

Public Security Vulnerability Data Sources (Examples)

Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
NIST National Institute of Standards and Technology

http://nvd.nist.gov/

NVD contains:

66963 CVE Vulnerabilities
254 Checklists
248 US-CERT Alerts
4308 US-CERT Vuln Notes
10286 OVAL Queries
98212 CPE Names

Last updated: 11/20/2014 10:08:05 AM

IPA Better Life with IT 情報処理推進機構

http://www.ipa.go.jp/security/english/

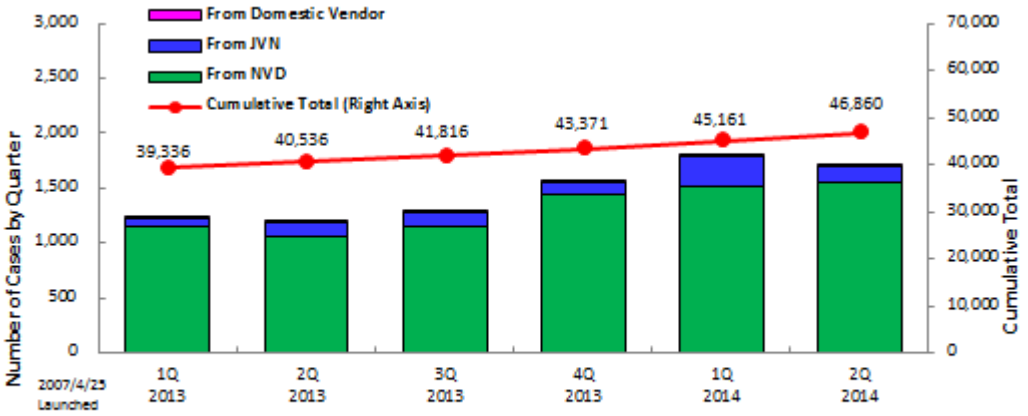


Figure 1-1. Quarterly Change in Number of Vulnerabilities Registered

http://www.osvdb.org/

OSVDB | Search OSVDB | Vendors | Project Info | Help OSVDB! | Sponsors | Account

Open Sourced Vulnerability Database

OSVDB's goal is to provide accurate, detailed, current, and unbiased technical security information.
The project currently covers **113,351** vulnerabilities, spanning **158,442** products from **4,735** researchers, over **112** years.

Business Risks of FOSS Deployment

Legal

- Non-compliance with FOSS license terms may lead to:
  - Preliminary Injunctions, delivery stops
  - Damage payments and profit skimming
  - Unfair competition claims
  - Criminal charges
- Copyleft risks
- Patent & trademark risks
- FOSS specific aspects
  - FOSS can be obtained without purchasing/legal involvement
  - License obligations come „unexpectedly“
  - FOSS license obligations are „unusual“ compared to commercial software

Mobile Computing Changes the Game

- Financial institutions are suddenly software distributors/vendors

- Additional license obligations kick in, e.g.
  - Provision of the license text
  - Provision of the source code
  - Attributions
  - Copyleft

BearingPoint

Business Risks of FOSS Deployment

Legal

Mature financial institutions actively manage FOSS compliance by…

… define legal entry gates for FOSS

… collecting and maintaining license information for all FOSS files

… examining all source code (own or delivered) for hidden FOSS

… keeping track meticulously where which FOSS is deployed

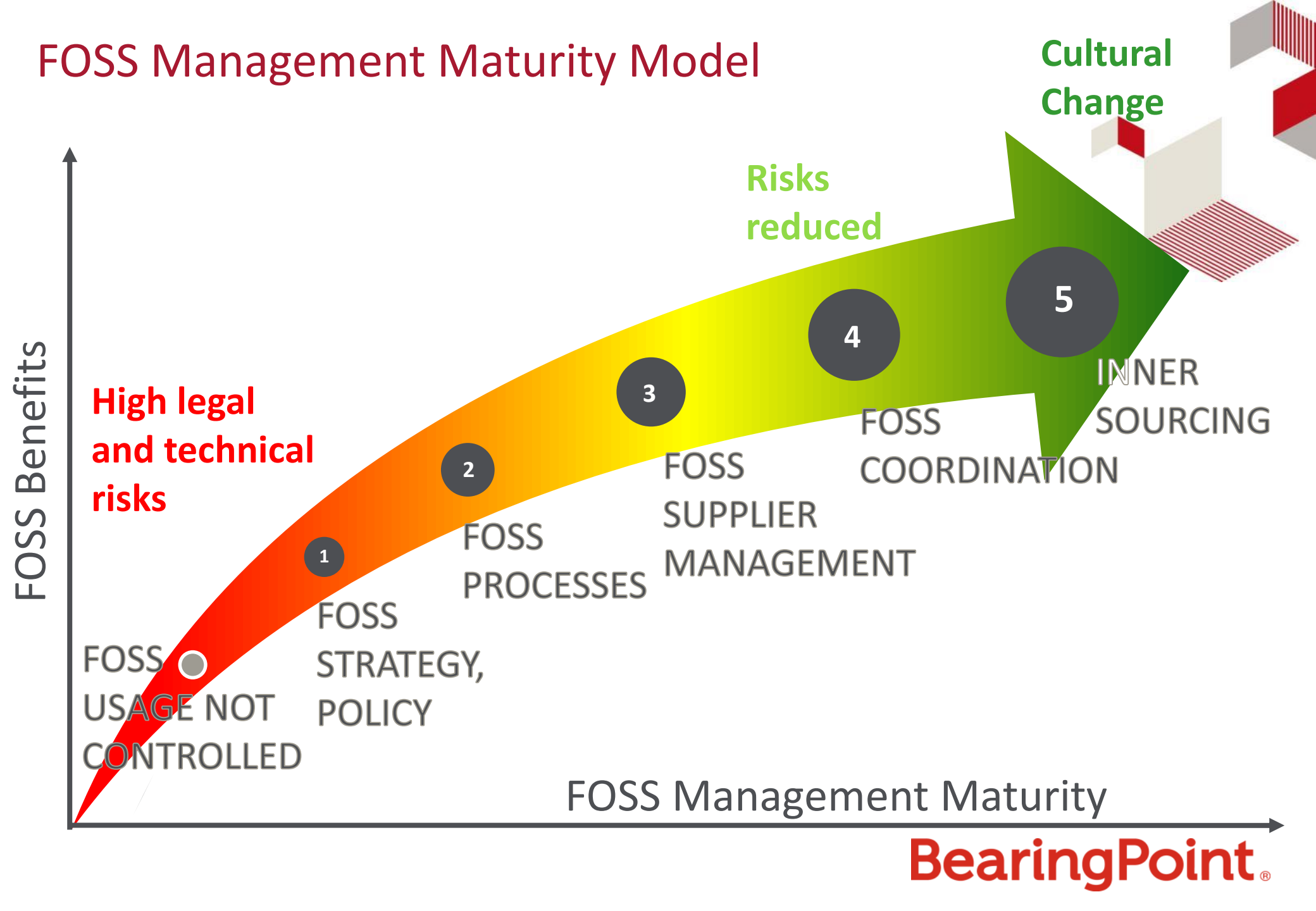
… accurately fulfilling all license obligations

… requiring all their suppliers to do the same

Use proper tooling. Manual attempts will fail.

Outsource to experienced supplier

FOSS Management Maturity Model



BearingPoint®

The FDIC says…

The use of FOSS is increasing in the mainstream information technology (IT) and financial services communities.The agencies believe that the use of FOSS does not pose risks that are fundamentally different from the risks presented by the use of proprietary or self-developed software.However, the acquisition and use of FOSS necessitates implementation of unique risk management practices.

Source: https://www.fdic.gov/news/news/financial/2004/FIL11404a.html

FOSS is not only software …

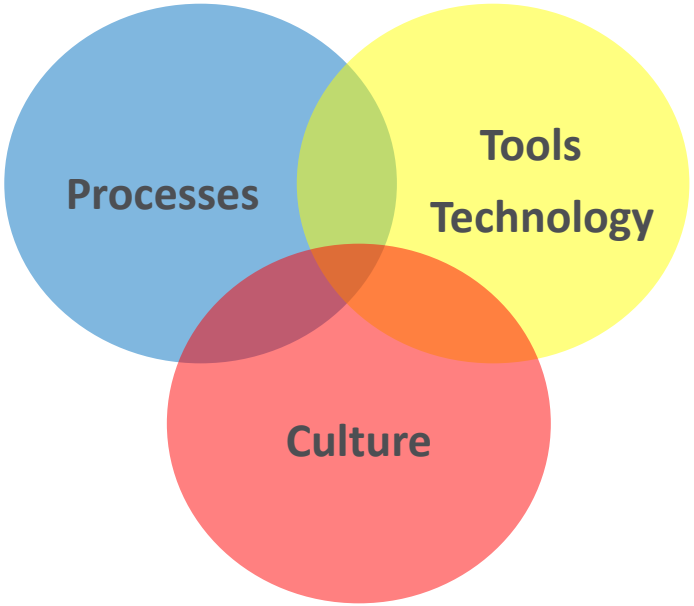
… but also a fundamentally different approach to software development and collaboration

FOSS Community Principles

- Transparency
- Collaboration
- Self-organization
- Meritocracy / voluntariness
- Iterative Release

Inner Sourcing is …

… the application of FOSS community principles and culture to internal software development and innovation efforts in order to bring them to the next level of performance.



Inner Sourcing is the Missing Link to …

… Better code

… Increased (internal & external) re-use

… Higher innovation velocity

… Faster development

… Reduced costs

… Higher attractiveness and retention

Mature financial institutions start Inner Source Programs to initiate sustainable culture change and software development performance improvement

Q & A

Contact

BearingPoint

Claus-Peter Wiedemann
Senior Manager

BearingPoint
Erika-Mann-Str. 9
80636 München
Germany

T +49 89 54033 6367
F +49 89 54033 7940
M +49 172 2757415

www.bearingpoint.com

claus-peter.wiedemann@bearingpoint.com

BearingPoint®