WG3 Status Report
15th NEAOSS Promotion Forum

Study on Standardization and Certification
Working Group of NEA OSS Promotion Forum

Cheju, Korea, 2016-11-16

Table of Contents

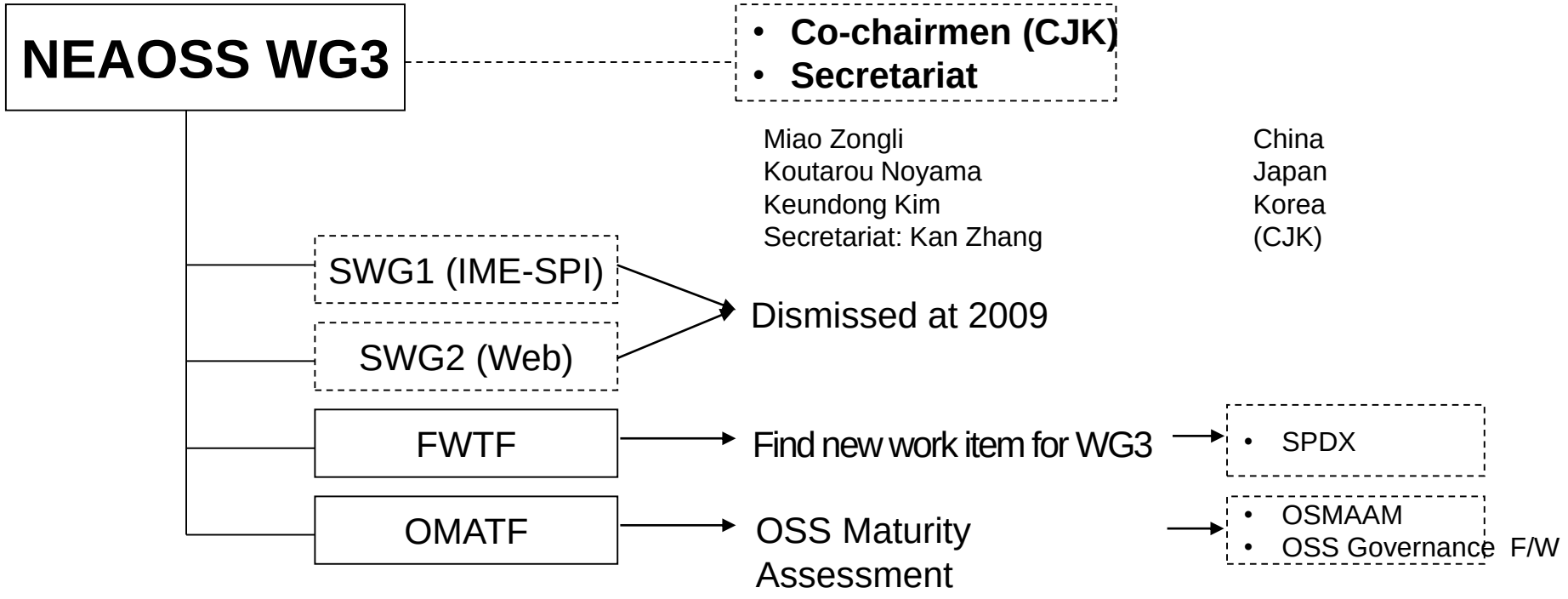
Introduction-Role of WG3

NEAOSS Forum formed

“WG3: Standardization and Certification Study” in order to study

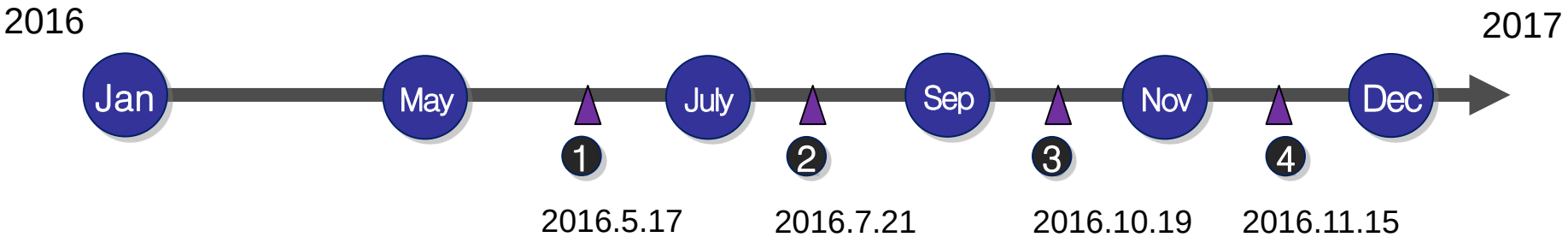
Open Source Software standardization and certification in July 2004

WG3 structure and Officers



❖ Note: All activities/decisions are per NEAOSS WG3 directives

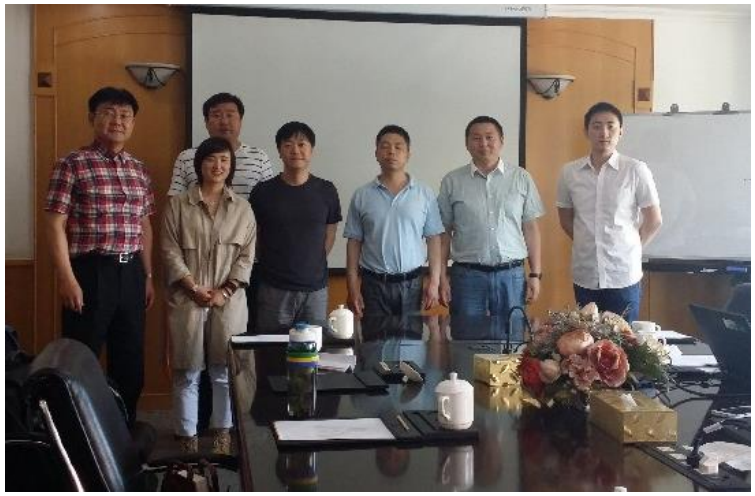
Recent Meeting Activities

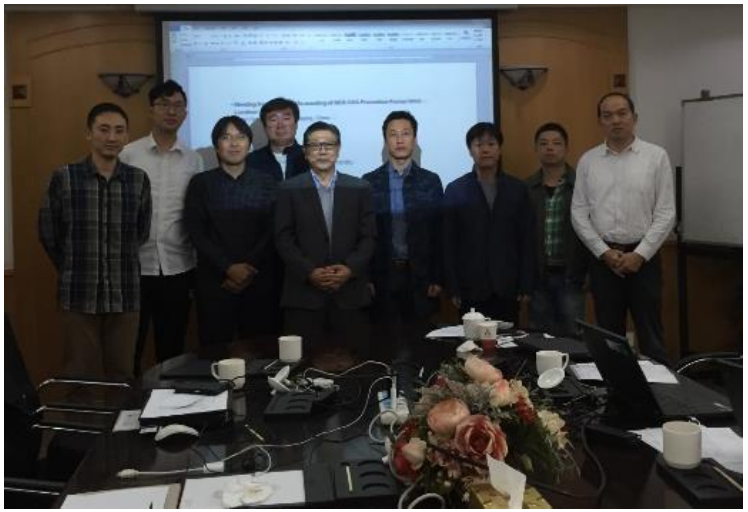


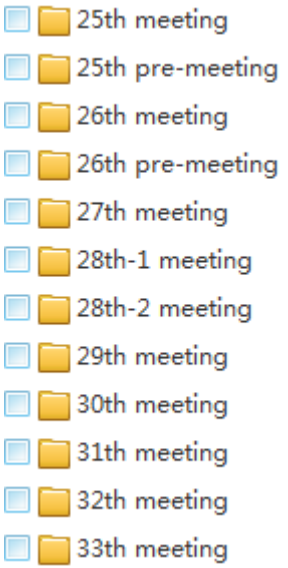
1	Beijing	• Evaluation Methodology of Government R&D Project • FOSS Supply Chain Risk Management • Open Source Software Hub
2	Tokyo	• Survey of OSS in Big Data Platform and Data Analysis Result • FOSS Supply Chain Risk Management • Standard Status of Smart terminal
3	Beijing	• Introduction of the OpenTHOS • FOSS Governance Guide • OASIS(Open Adoption Support Information System)
4	Cheju	• Preparation for 15th NEA OSS Promotion Forum • WG3 Work Plan in 2017

WG3 Documents Server

- Totally：
  - WG3 Meeting: 38
  - WG3 Documents: 276



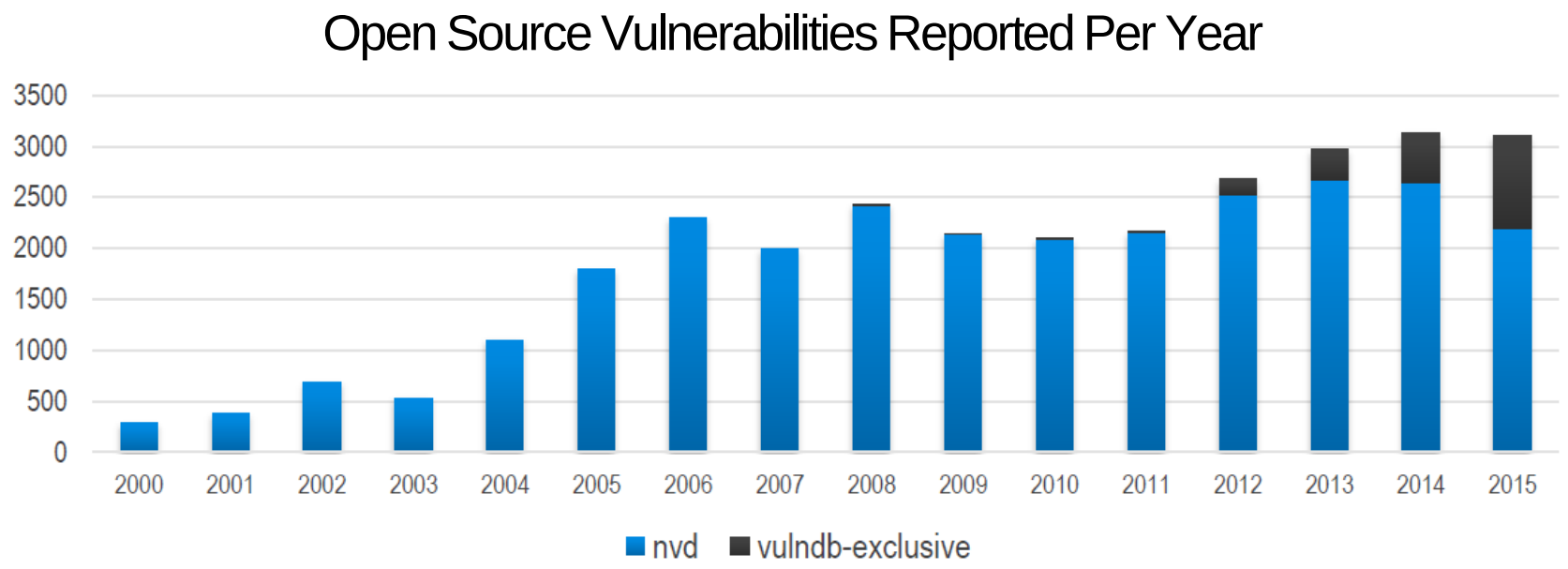




FOSS Supply Chain Risk Management

Background

- “By 2016, Open Source Software will be included in mission-critical applications within 99% of Global 2000 enterprises.” Gartner, Inc.
- “78% of companies run on open source software.” 2015 the future of open source



Reference: Black Duck Software knowledgebase, NVD, VulnDB

FOSS Supply Chain Risk Management

	Heartbleed	Shellshock	Freak	Ghost	Venom
Component:	OpenSSL	Bash	OpenSSL	GNU C library	QEMU
Introduced:	2011	1989	1990's	2000	2004
Discovered:	2014	2014	2015	2015	2015
Found by:	Riku, Antti, Matti, Mehta	Chazelas	Beurdouche	Qualys researchers	Geffner

FOSS Supply Chain Risk Management

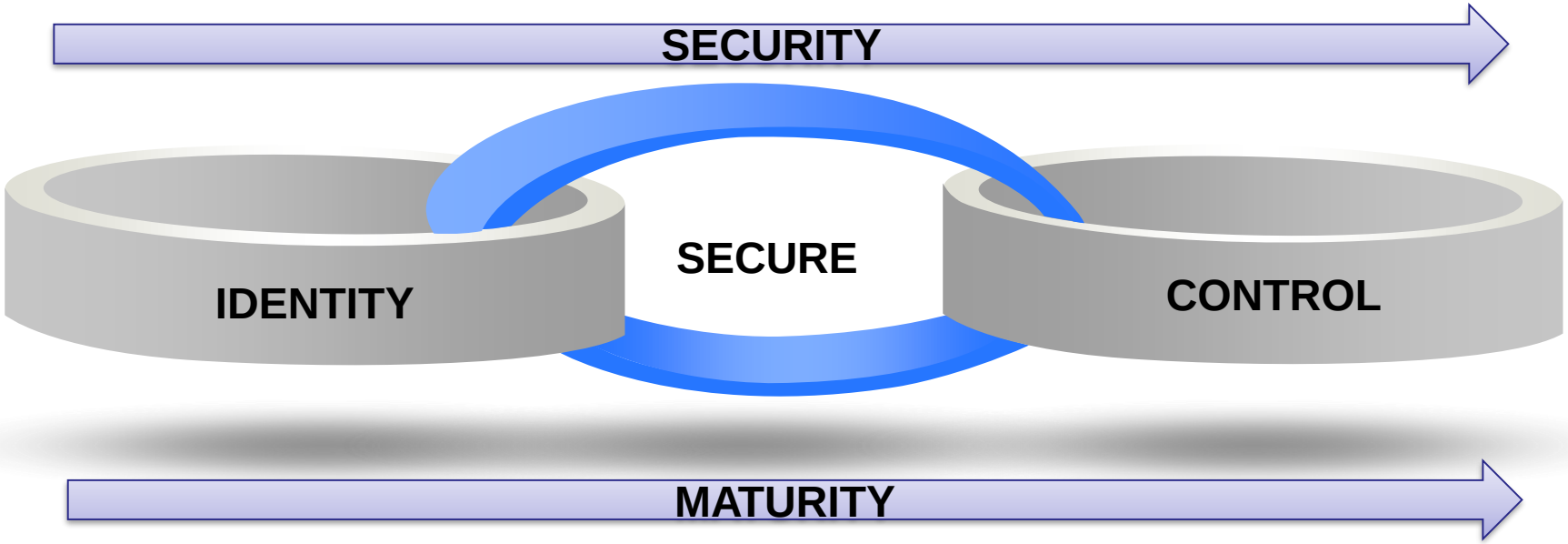
- **Why Legal Teams Care about Open Source Security?**
- Open source risk management is not limited to license compliance.
- Legal teams are increasingly aware of security obligations & risks.

- **Internal/External Reporting**
  - Executive management, Directors, Regulatory Agencies
- **Litigation Risks**
  - Lawsuits from customer/patient/financial data loss
- **Regulatory Penalties**
  - HIPAA, PCI, SOX
- **Loss of company IP/secrets**
- **Damage to company reputation from high-visibility breaches**

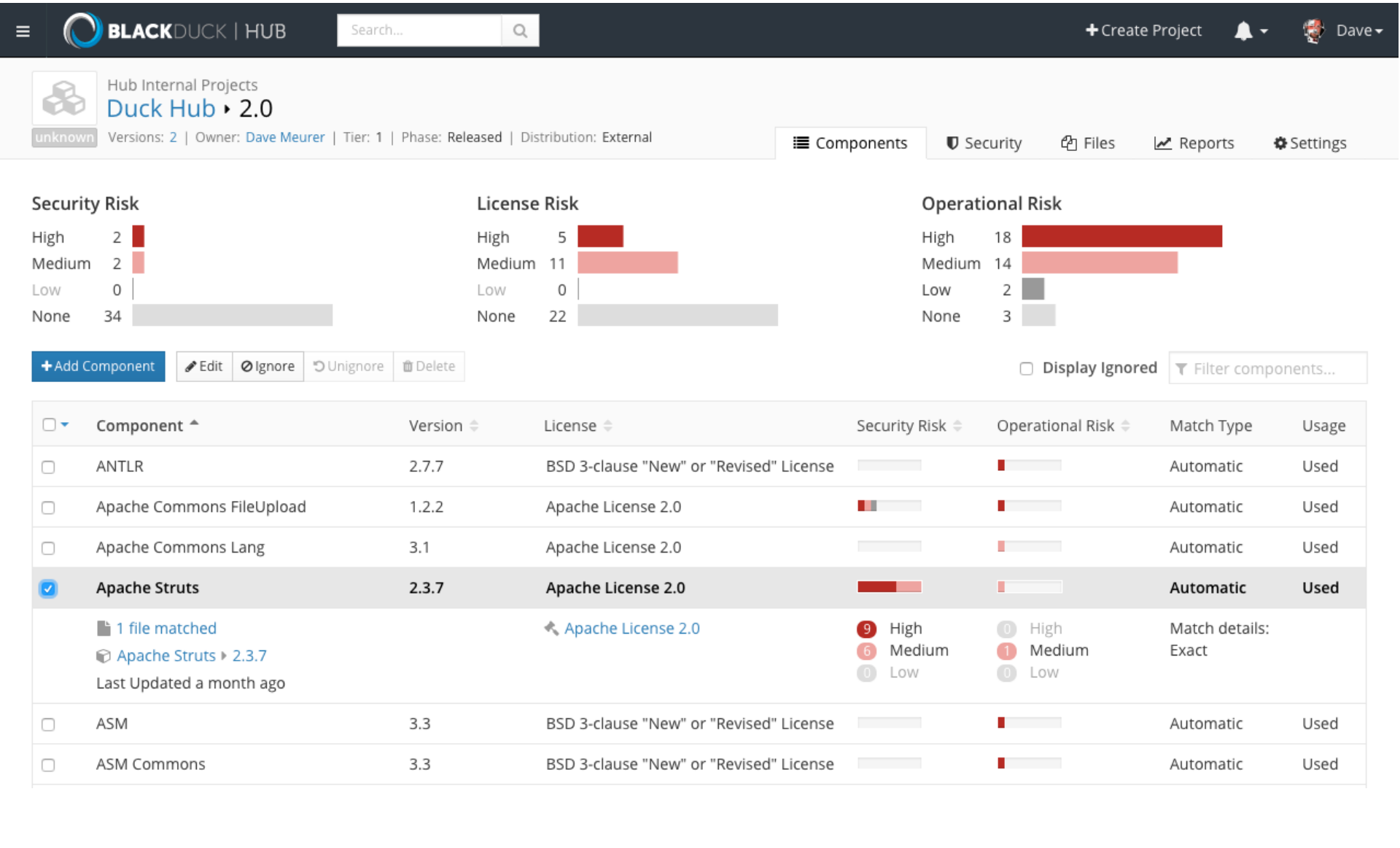
FOSS Supply Chain Risk Management

- **Four factors that make open Source different**
  1. **Used everywhere**
  2. **Easy access to code**
  3. **Vulnerabilities are public**
  4. **Exploits readily available**

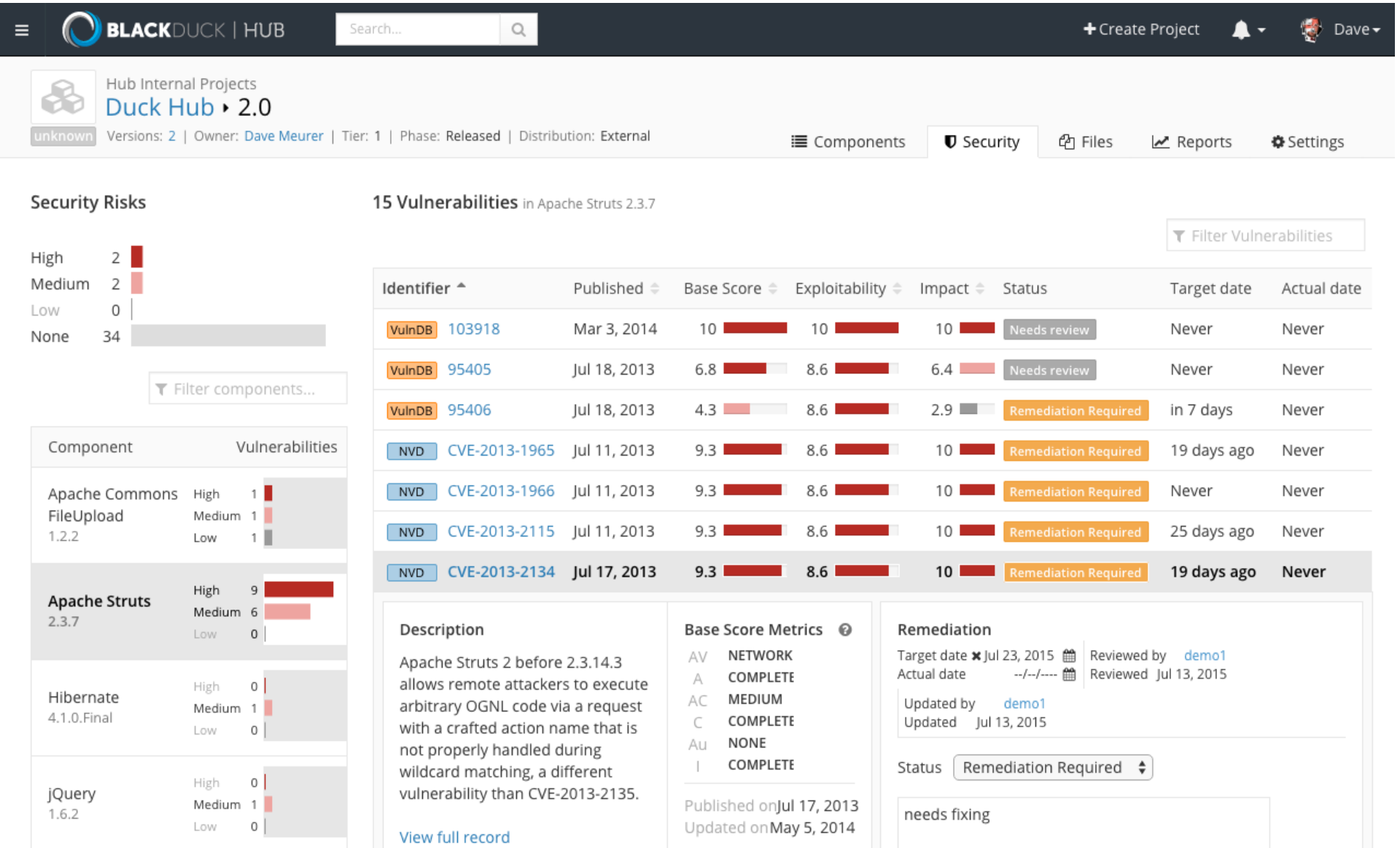
- **The Road to Secure Open Source Use**



FOSS Supply Chain Risk Management



FOSS Supply Chain Risk Management



FOSS Supply Chain Risk Management

Classification	Standard Development Organisation	Standard	Comments
1 Origins (sources) of supply chains	ISO SC27	ISO/IEC 27036: Guidelines for Security of Outsourcing	These are generic documents and not specific to SCI
2 Delivery and governance of the Supply Chain	NASPO (North American Security Products Organization) NIST		Nothing specific to SCI
3 Processing and configuration	ISO SC31 iNEMI Supply Chain study group HDPUG Supply Chain study group:	RFID supply chain applications Risk Modelling pilot Data Exchange pilot	Nothing specific to SCI
4 Integrity techniques	JTC1-SC27 Safecode Open Group	N10656: Update to ISO 27002: Security Techniques Open Trusted Technology Framework	Nothing specific to SCI
5 Verification and checks	ISO TC247	Fraud Controls and Countermeasures SEMI T20: Traceability (semiconductor industry)	Nothing specific to SCI

FOSS Supply Chain Risk Management

- WG3 has finished **FOSS SCRM standard guideline**
  - The requirements of OSS supply management
  - The governance for OSS SCRM
  - OSS profiling for SCRM
  - The guide of compliance for SCRM
  - SPDX Specification
  - The application of SPDX for SCRM

We have supplied service for more than **1000** enterprises.

목 차

FOSS Governance

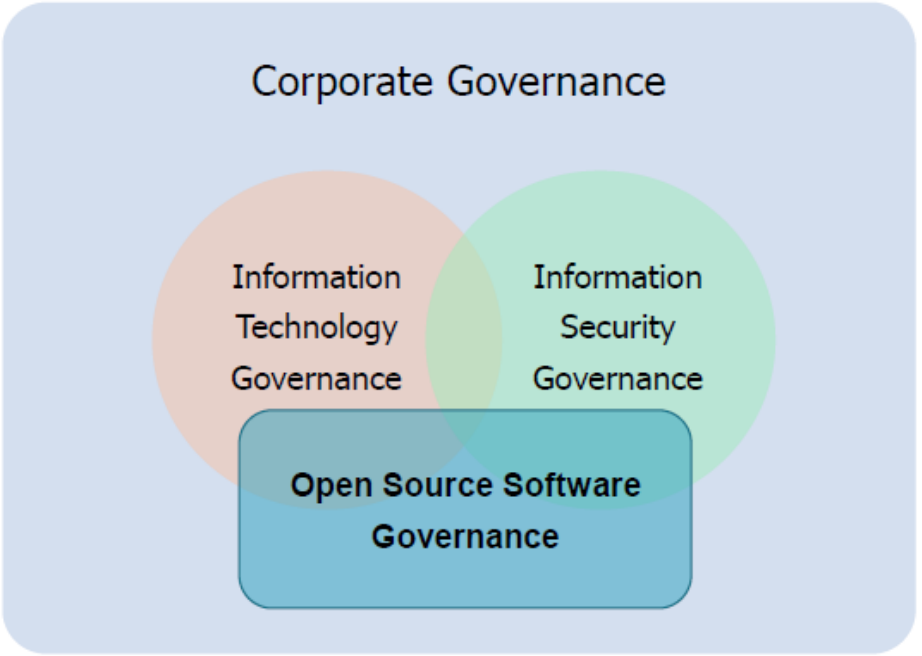
- **Definition**
  - Open-source governance (also known as open politics) is a **political philosophy** which advocates the application of the philosophies of the open-source and open-content movements to democratic principles to enable any interested citizen to add to the creation of policy, as with a wiki document. (https://en.wikipedia.org/wiki/Open-source_governance)

  - Open source governance is the way an organization controls the use of open source software within their products and services, supply chains and business management activities, and the associated business and legal processes. (blackduck)

FOSS Governance

- **Purpose**
  - This guide provides a control framework and procedures for companies using open source, designed to help the accountability and compliance of enterprise open source.

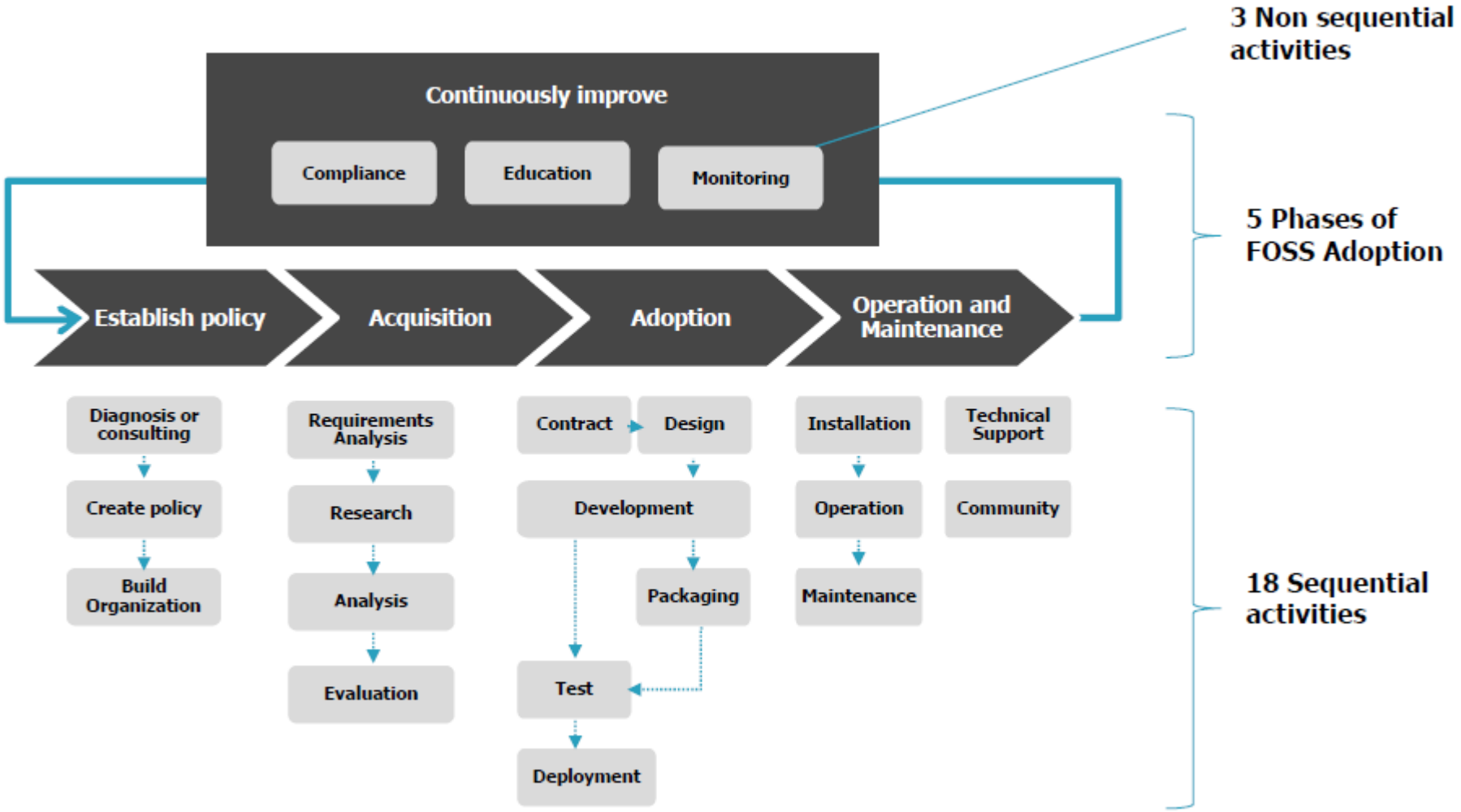
- **Scope**



Scope of open source governance

FOSS Governance

- **Structure of FOSS Governance framework**



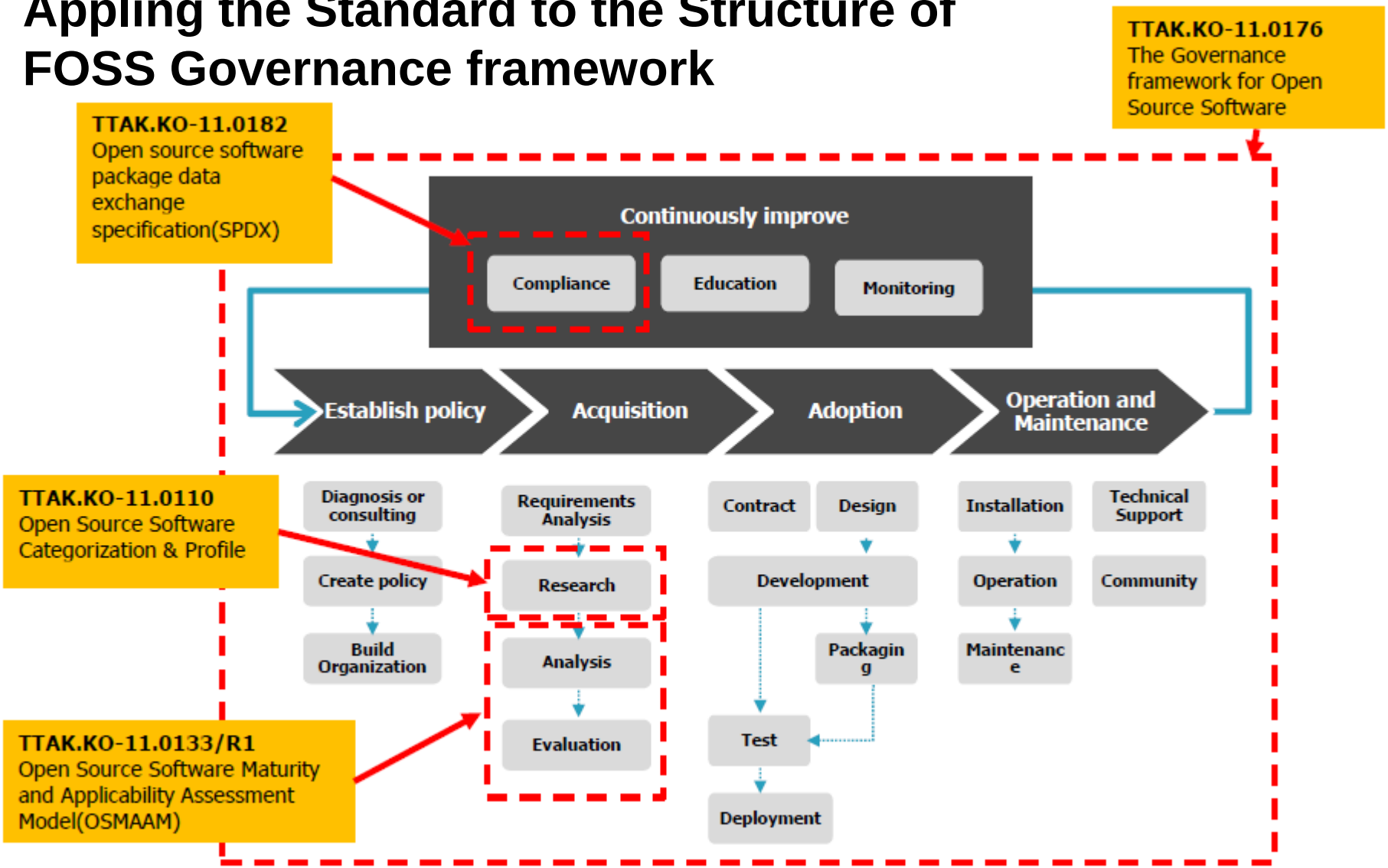
FOSS Governance

- **Four standards in Korea**

No.	Name of the Standard
TTAK.KO-11.0110	Open Source Software Categorization & Profile
TTAK.KO-11.0133/R1	Open Source Software Maturity and Applicability Assessment Model(OSMAAM)
TTAK.KO-11.0182	TTAK.KO-11.0182 Open source software package data exchange specification(SPDX)
TTAK.KO-11.0176	The Governance framework for Open Source Software

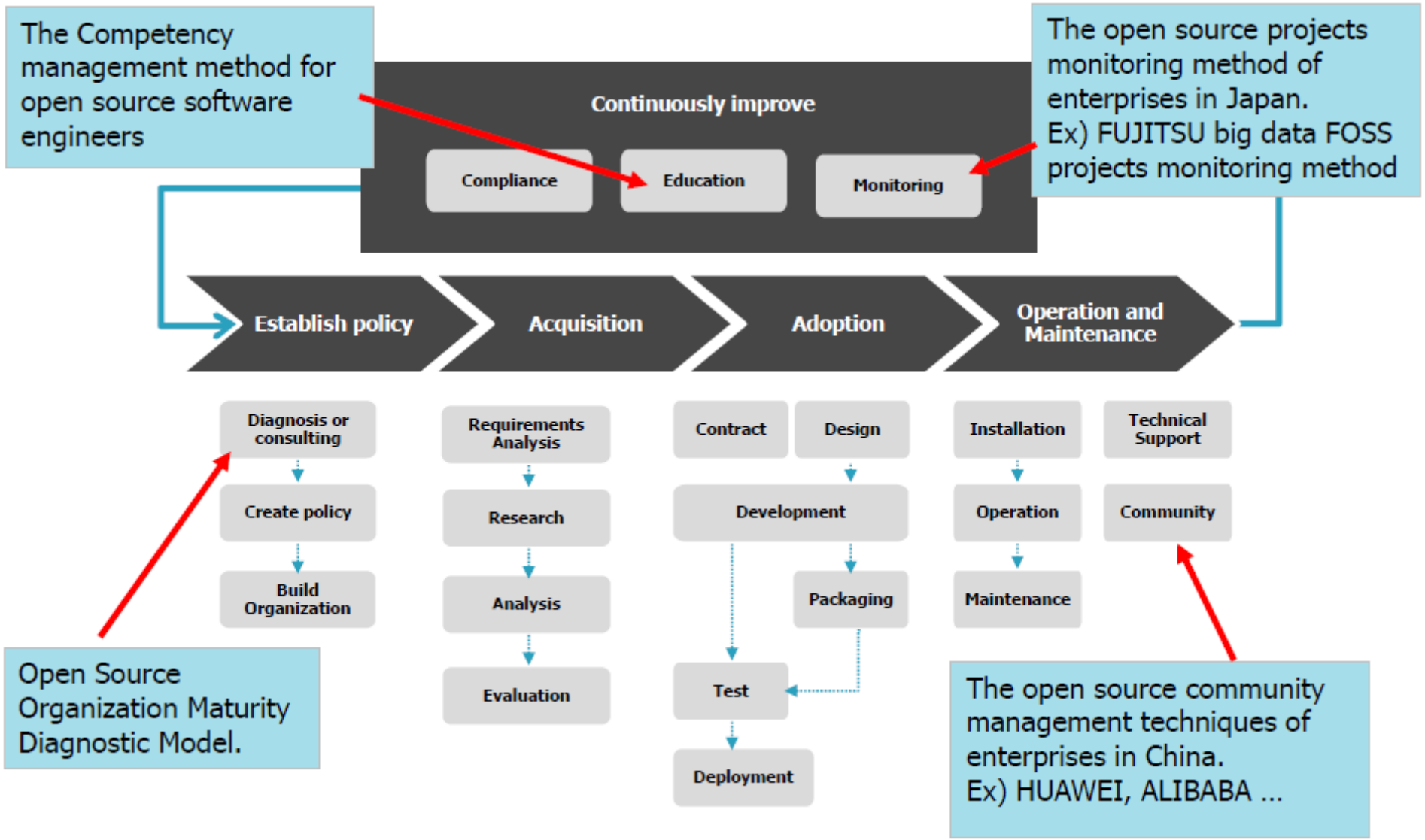
FOSS Governance

- **Appling the Standard to the Structure of FOSS Governance framework**



FOSS Governance

- **Future Work Overview**



Technology requirement of mobile terminal browser

- **Background**

  PC：interactive terminal ＝2:3（2007）

  PC：smart terminal ＝1:10（Now）

  smart terminal will reach 33 billion in 2020 ≈ 4.3 / person

- **Purpose**
  - This standard applies to the design, development and test of mobile terminal browser

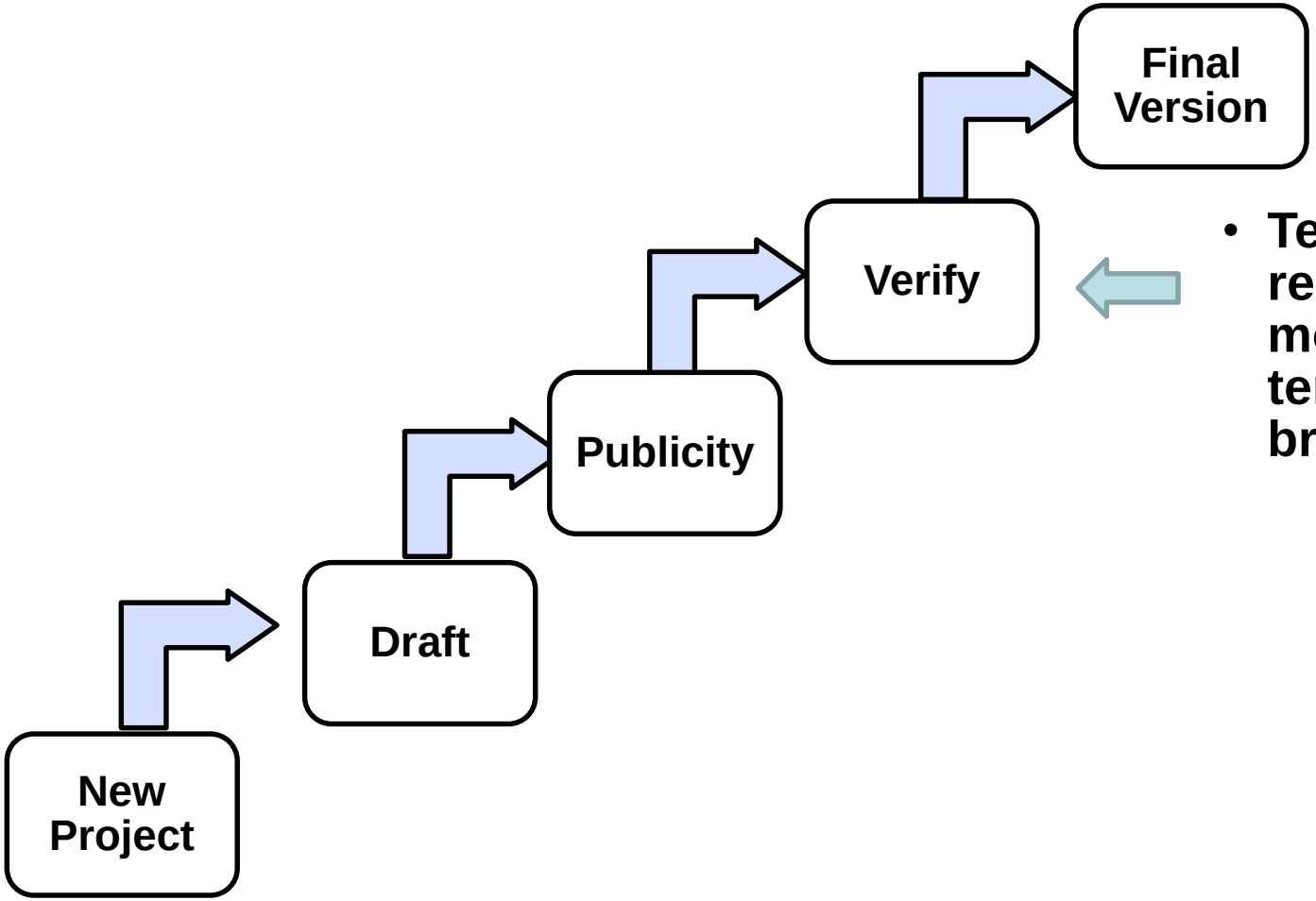
Technology requirement of mobile terminal browser

- **Scope**

Run-time System Requirements	Protocol Requirements	Function Requirements	Software Design Requirements
• Network • Platform • Memory • Screen • Keyboard • Input Method • …	• Makeup Language • Transfer Protocol • Security Protocol • Image Format • Audio and Video Format • Cache • …	• Display • Operation • Network • Address Bar Function • Download Function • Upload Function • Bookmark Function • Security Function • Cache Function • …	• Design Rules • Analytical Page Requirements • Performance Requirements • Core Requirements • Cache Requirements • …

Technology requirement of mobile terminal browser

- **Standard Status**



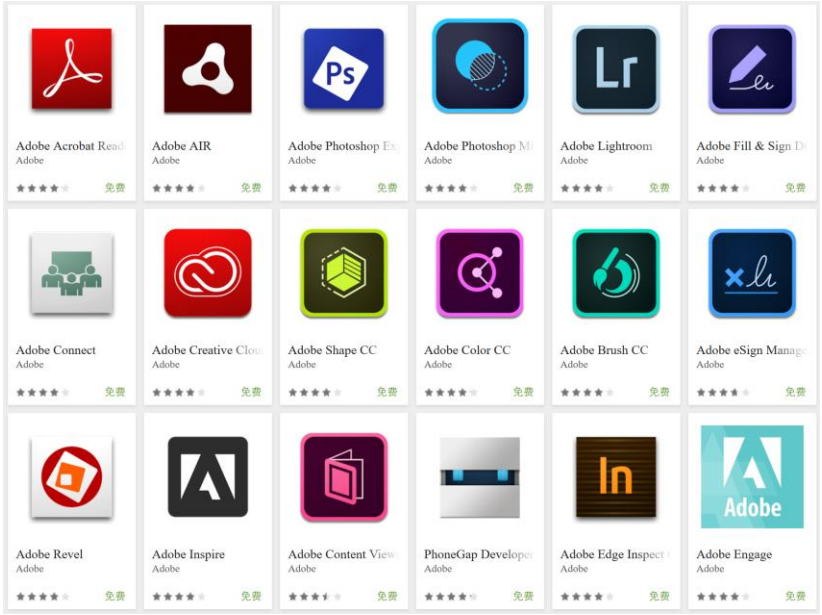
- **Technology requirement of mobile terminal browser**

OPENTHOS

- Background
- Problem
- What
- How
- Purpose

OPENTHOS

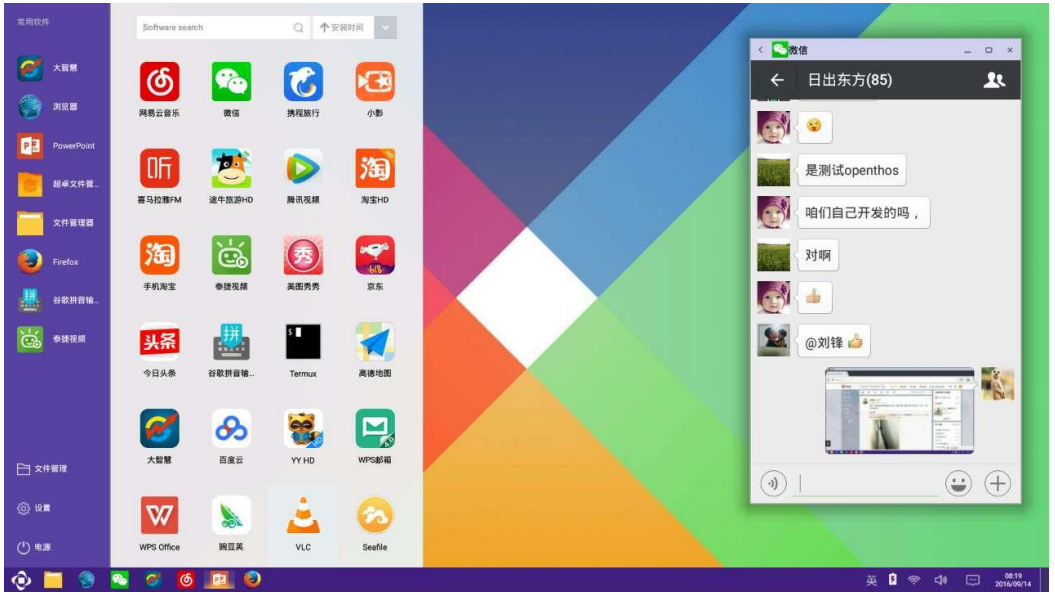
- **Purpose**
  - **High performance OS**
  - **Android ecosystem**
    - **Developers**
    - **User**
  - **High Security**
  - **Cross-platform**



OPENTHOS

OPENTHOS

- **Characters**
  - **Multi-Windows Mngt**
  - **Phone & Pad supported**
  - **Mouse & Touch supported**
  - **Print supported**
  - **High performance**
    - **60 frames/second**
    - **Low delay**
  - **Low hardware requirement**
  - **Unitive user information**
    - **Real-time backup**
    - **Synchronization between devices**
    - **High security**
    - **High reliability**
  - **OPENThos Cloud**



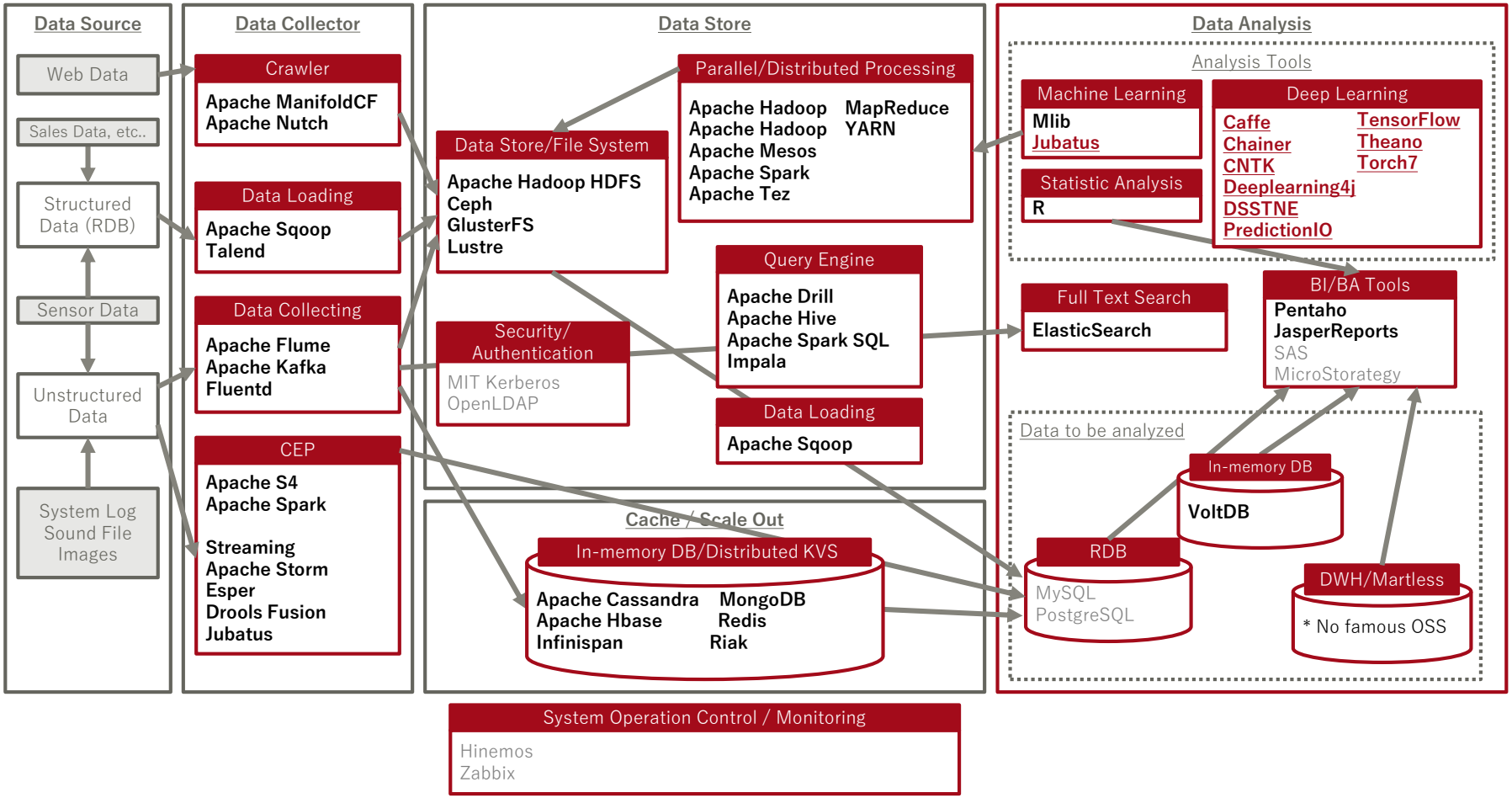
OPENTHOS

OPENTHOS

- Community
  - Committers
    - Tinghua
    - Tongfangpc
    - emindsoft
    - …
- Status
  - IOS version available
    - Download : 700 in August
  - Source Code
    - https://github.com/openthos
  - 2016.12 - release on Tongfang PC

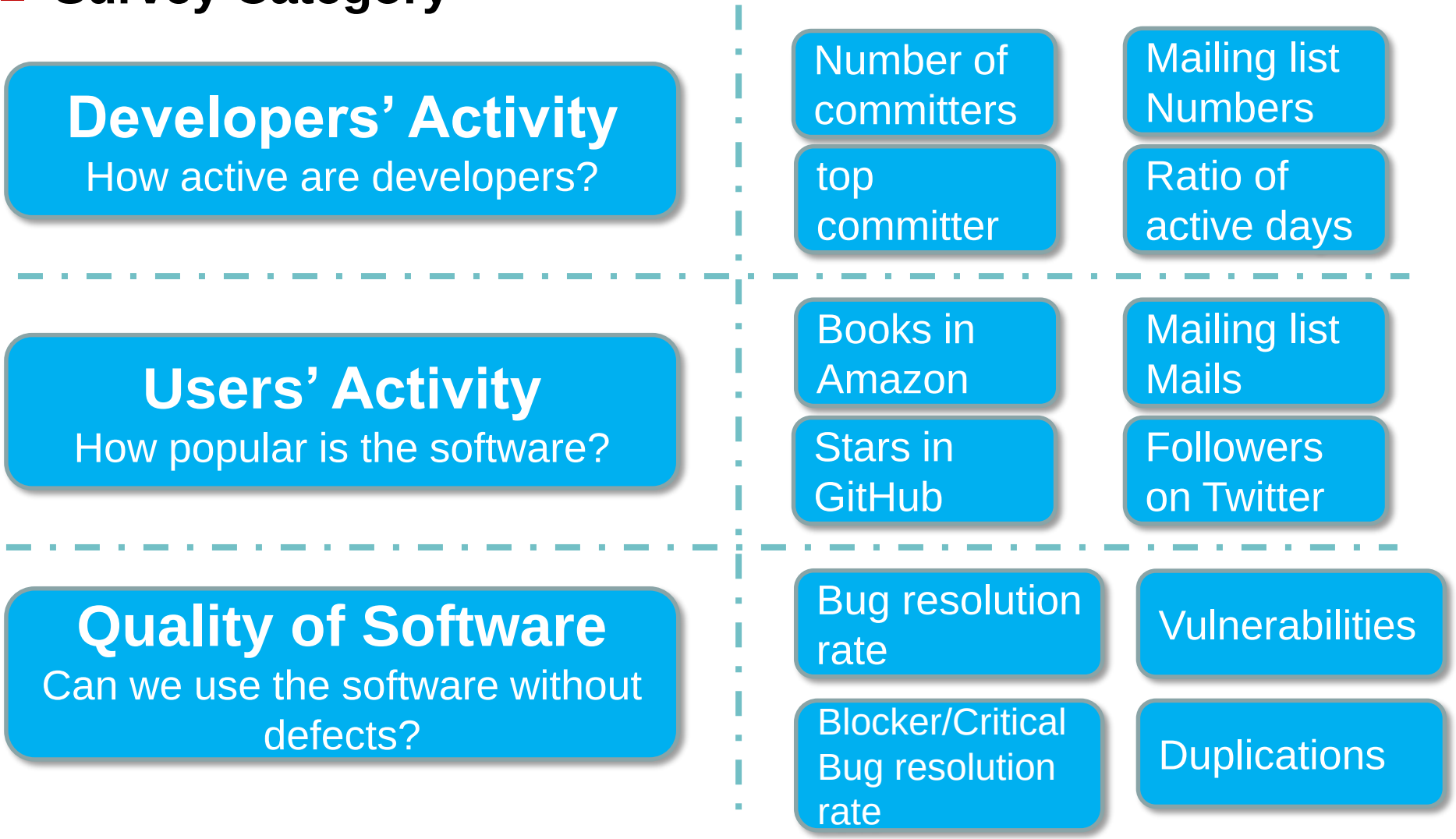
Survey of OSS in Big Data Platform

- **Structure**



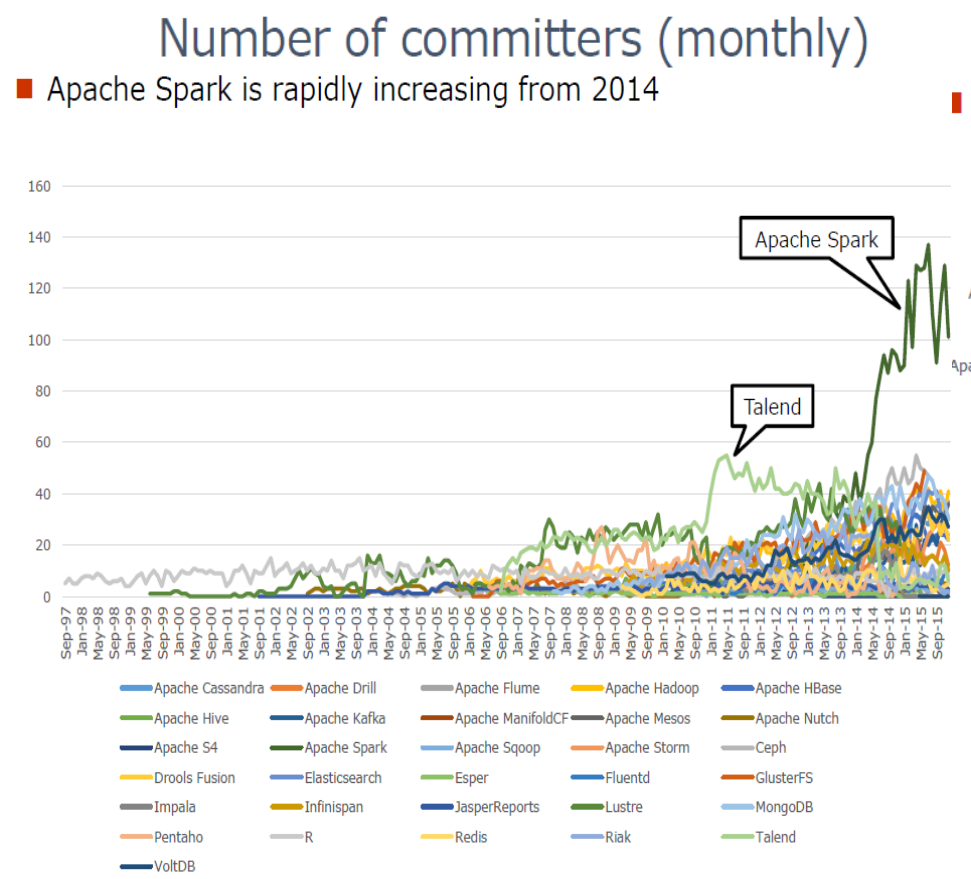
Survey of OSS in Big Data Platform

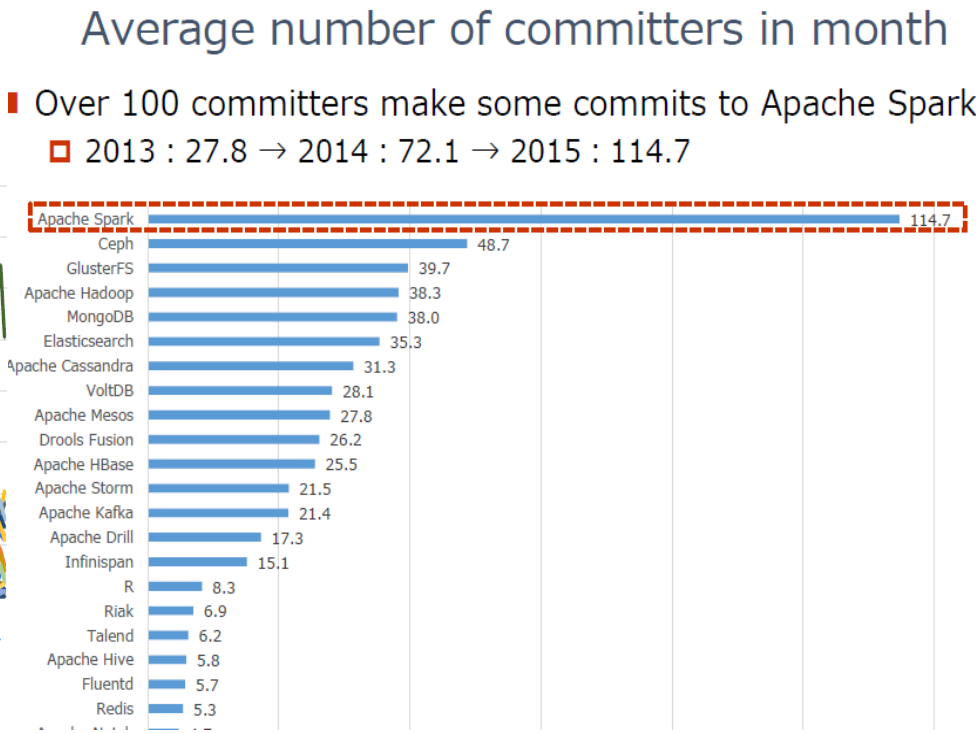
- **Survey Category**



Survey of OSS in Big Data Platform

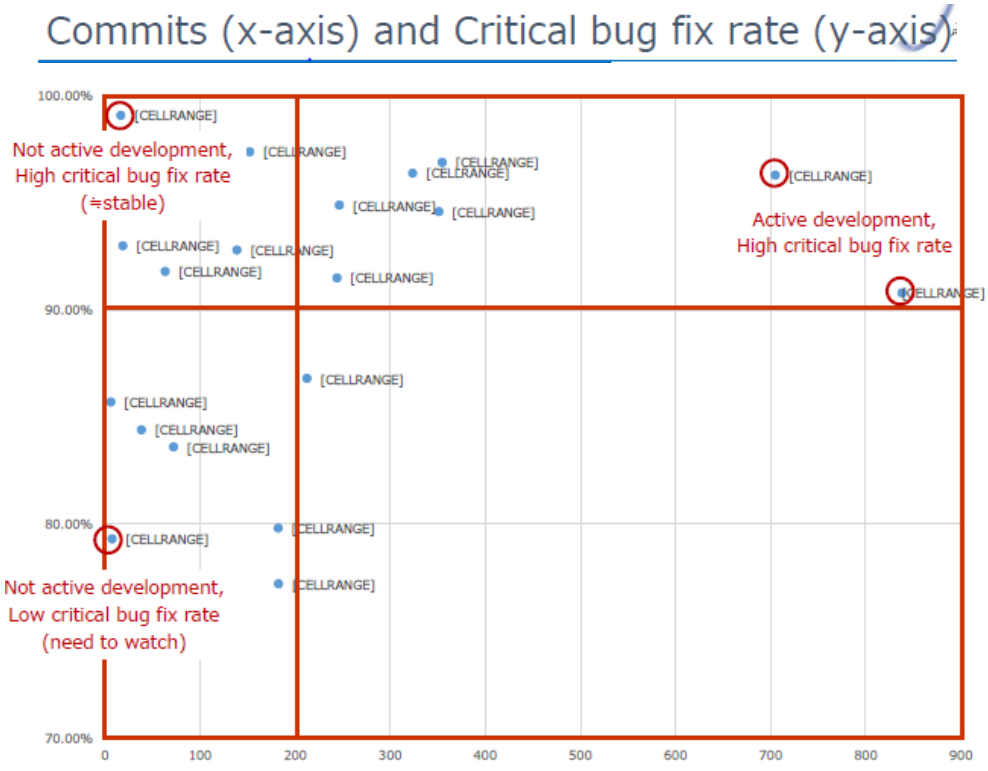
- **Survey Result**

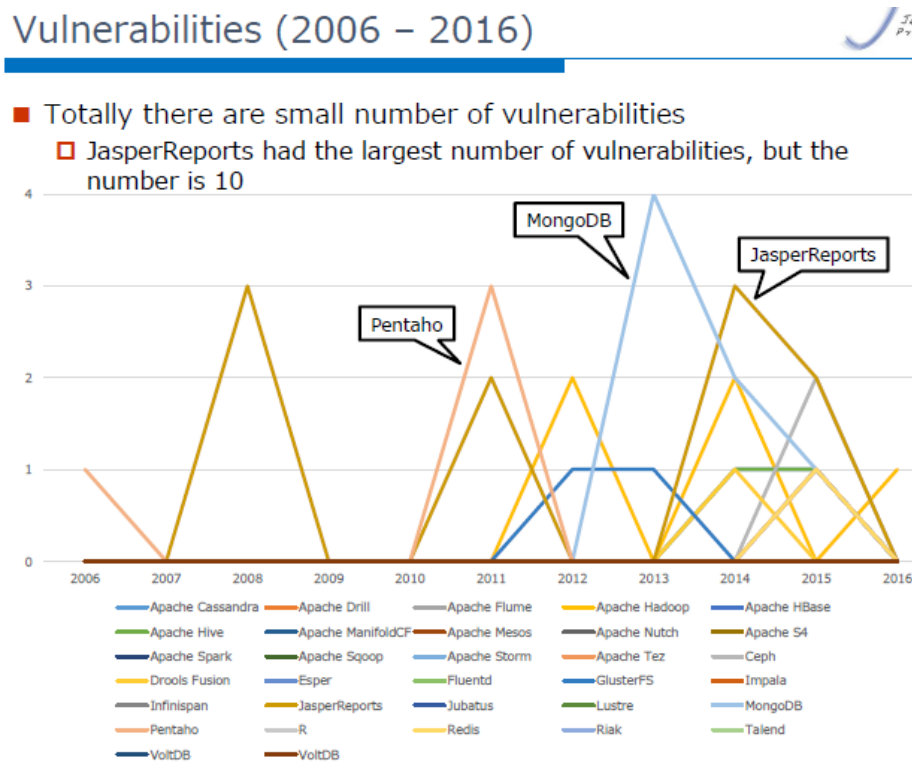




Survey of OSS in Big Data Platform

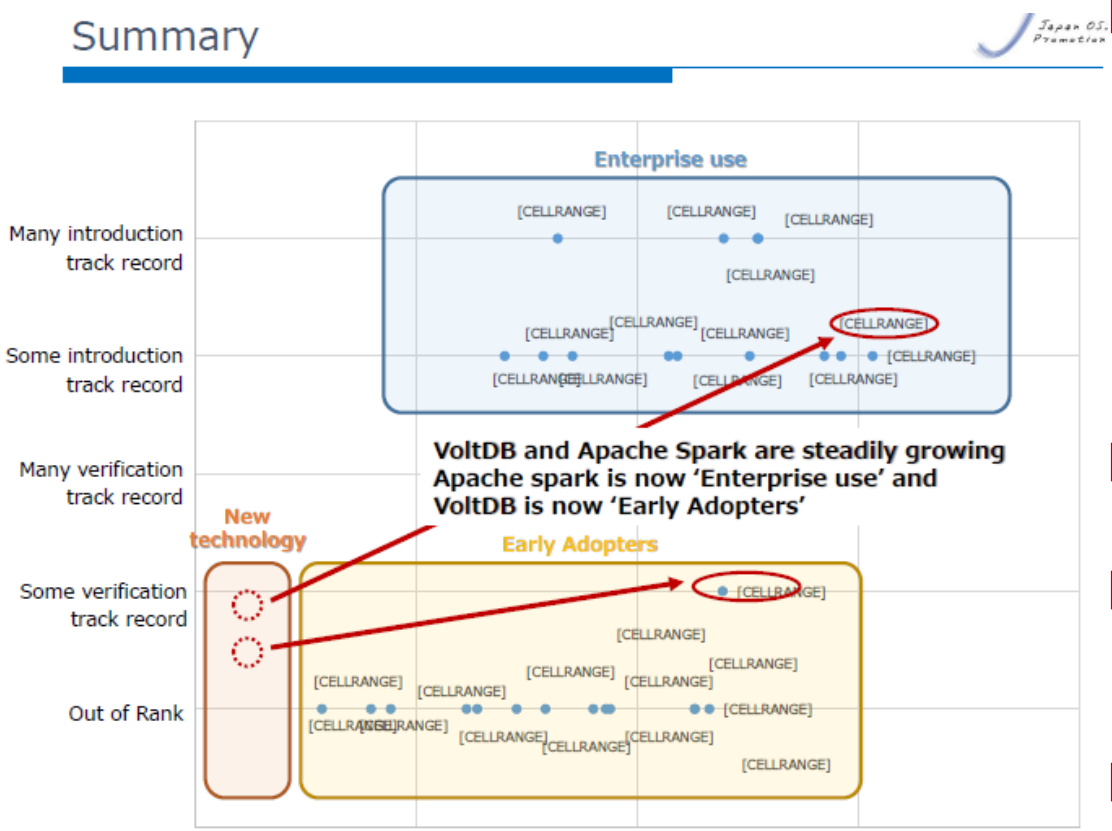
- **Survey Result**





Survey of OSS in Big Data Platform

Survey Summary



Survey Conclusion

- We can build the Big Data Platform only with OSS
  - Enterprise supports are getting better
  - However, it is necessary to check the functions and quality of softwares
- Apache Spark and the ecosystem are **hot**
- Developers for Elasticsearch may be **hardworkers**
- MongoDB and Ceph are going to be **stable**

Work Plan of WG3 in 2017

- OASIS(Open source Support Information System)
- Assessment Model of Open R&D project for Government
- Applying FOSS Supply-Chain Risk Management Guide
- OpenTHOS Project
- Promote the application of WG3 achievements in CJK.

Thank you very much!

谢谢

ありがとうございました

감사합니다